ÁLGEBRA LINEAR I

$2^{o.}$ SEMESTRE DE 2024

EXERCÍCIOS

Entrega. Entregue suas soluções no e-Disciplinas.

Política de colaboração e uso de fontes. Todo trabalho entregue por você deve ser seu. Você é encorajado a discutir com seus colegas o material visto em sala e os enunciados dos exercícios, mas tome cuidado para não compartilhar seu trabalho além do permitido. Nos *exercícios individuais*, você não pode compartilhar suas soluções ou mesmo ideias de soluções. Nos *exercícios em grupo*, você só pode compartilhar suas ideias e soluções com membros de seu grupo. Nos exercícios em grupo, *cada membro do grupo deve escrever uma solução própria.* Ao entregar um exercício feito em grupo, não esqueça de escrever o nome de todos os membros do grupo em sua solução.

Você não deve procurar soluções de terceiros (como de amigos ou na Web). Caso você acidentalmente encontre e leia a solução de algum exercício em algum lugar, você deve citar esta fonte em sua solução. Caso você acidentalmente acabe colaborando com colegas na descoberta de uma solução, você deve citar esta colaboração em sua solução. Seu desempenho nesta disciplina ficará prejudicado caso você viole essas regras.

Fontes dos exercícios. Vários dos exercícios vêm de nossa bibliografia. Usamos as seguintes abreviaturas (outras abreviaturas poderão ser adicionadas posteriormente). **PNK:** Philip N. Klein, *Coding the matrix*; **SA:** Sheldon Axler, *Linear algebra done right* (3a edição).

Exercícios para entrega. Os exercícios para entrega estão marcados com uma data de entrega e são em geral individuais. Os exercícios que podem ser feitos em grupo estão claramente marcados dessa forma, e o número máximo de alunos por grupo está especificado.

Exercícios marcados (M). Os exercícios marcados (M) são para os mais matematicamente inclinados, e não serão cobrados nessa disciplina.

* * * * *

E1 Faça o Problema 0.8.3 de **PNK**.

E2 Faça os Problemas 0.8.4 e 0.8.11 de **PNK**.

E3 Sejam A e B conjuntos. Seja $\mathcal{P}(A) = \{S\colon S \subset A\}$ o conjunto dos subconjuntos de A (o *conjunto potência* de A ou *conjunto das partes* de A). Lembre que B^A é o conjunto das funções $f\colon A \to B$. Considere a função $F\colon \mathcal{P}(A) \to \{0,1\}^A$ tal que, para todo $S \in \mathcal{P}(A)$, temos

$$(F(S))(a) = \begin{cases} 1 & \text{se } a \in S \\ 0 & \text{caso contrário.} \end{cases} \tag{1}$$

Prove que F é bijetora. [*Observação.* A função $F(S)$ é conhecida como a *função característica* de S. É comum denotar $F(S)$ por $\mathbb{1}_S$ ou χ_S.] **{*Data de entrega*: 22/8/2024}**

Date: Versão de 2025/1/20, 9:12pm.

E4 A *diferença simétrica* $A \triangle B$ dos conjuntos A e B é o conjunto $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Prove que a operação de diferença simétrica é associativa, isto é, que $A \triangle (B \triangle C) = (A \triangle B) \triangle C$ para quaisquer conjuntos A, B e C. [*Sugestão.* Seja U um conjunto tal que $A \cup B \subset U$, e considere as funções características $\mathbb{1}_A$ e $\mathbb{1}_B$ de A e B como vetores em $\mathrm{GF}(2)^U$ (lembre-se do Exercício **E3**). O que é o vetor $\mathbb{1}_A + \mathbb{1}_B \in \mathrm{GF}(2)^U$?] **{*Data de entrega*: 22/8/2024}**

E5 Sejam A_i $(0 \le i < N)$ conjuntos e seja

$$B = A_0 \triangle \cdots \triangle A_{N-1} \tag{2}$$

sua diferença simétrica. Seja $I(x)$ a propriedade "há um número ímpar de índices i $(0 \le i < N)$ para os quais $x \in A_i$". Prove que

$$B = \Big\{ x \in \bigcup_{0 \le i < N} A_i \colon\ I(x) \Big\}. \tag{3}$$

E6 Complete a implementação de `vec.py`. Não deixe de executar `python -m doctest vec.py` para testar sua implementação.

E7 Faça o Problema 2.14.5 de **PNK**. No caso em que não há subconjunto de $\{\mathbf{a}, \dots, \mathbf{f}\}$ que tem como soma o vetor desejado, justifique sua resposta de forma elegante, considerando o produto escalar com o vetor 1011011.

E8 Seja $N \ge 2$ um inteiro. Consideramos aqui matrizes $N \times N$ com entradas em $\mathrm{GF}(2)$ e com as linhas e colunas indexadas por $\{0, 1, \dots, N-1\}$. Para cada $0 \le r < N-1$ e $0 \le s < N-1$, seja $B_{rs} = (b_{ij}^{(rs)})_{0 \le i,j < N}$, onde

$$b_{ij}^{(rs)} = \begin{cases} 1 & \text{se } (i,j) \in \{r, r+1\} \times \{s, s+1\}, \\ 0 & \text{caso contrário.} \end{cases} \tag{4}$$

Seja $A = (a_{ij})_{0 \le i,j < N}$, onde

$$a_{ij} = \begin{cases} 1 & \text{se } (i,j) \in \{0, N-1\} \times \{0, N-1\}, \\ 0 & \text{caso contrário.} \end{cases} \tag{5}$$

Finalmente, seja $A' = (a'_{ij})_{0 \le i,j < N}$, onde

$$a'_{ij} = \begin{cases} 1 & \text{se } (i,j) \in \{(0,0), (0, N-1), (N-1, 0)\}, \\ 0 & \text{caso contrário.} \end{cases} \tag{6}$$

Por exemplo, se $N = 3$, as 4 matrizes B_{rs} $(0 \le r, s < 2)$ são

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \tag{7}$$

Ademais,

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{e} \quad A' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \tag{8}$$

Prove as seguintes afirmações (lembre que estamos trabalhando sobre $\mathrm{GF}(2)$):

(i) Para qualquer $N \ge 2$, temos $A \in \mathrm{Span}\{B_{rs} \colon 0 \le r, s < N-1\}$.

(*ii*) Para qualquer $N \geq 2$, temos $A' \notin \mathrm{Span}\{B_{rs}\colon 0 \leq r, s < N-1\}$. [*Sugestão.* Veja o Exercício **E7** e considere a matriz $Z = (z_{ij})_{0\leq i,j<N}$ sobre GF(2) em que $z_{ij} = 1$ se e só se $i + j$ é par. Uma matriz mais simples que também serve é a matriz J sobre GF(2) em que todas as entradas são 1.]

***{Data de entrega*: 29/8/2024}**

E9 Sejam dados $\mathbf{a}_i = (a_{ij})_{0\leq j<n} \in \mathbb{F}^n$ $(0 \leq i < n)$ e $\mathbf{b} = (b_i)_{0\leq i<n} \in \mathbb{F}^n$ e considere o sistema de equações lineares

$$\begin{cases} \mathbf{a}_0 \cdot \mathbf{x} = b_0 \\ \qquad \dots \\ \mathbf{a}_{n-1} \cdot \mathbf{x} = b_{n-1}, \end{cases} \tag{9}$$

onde $\mathbf{x} = (x_j)_{0\leq j<n}$. Suponha ainda que, para todo $0 \leq i < n$, temos que $a_{ij} = 0$ para todo j com $j < i$, de forma que (9) é um sistema *triangular*.

Lembre que, se $a_{ii} \neq 0$ para todo $0 \leq i < n$, então (9) admite uma solução e essa solução é única. Prove que se existe um k com $0 \leq k < n$ tal que $a_{kk} = 0$, então existe um $\mathbf{b} = (b_i)_{0\leq i<n} \in \mathbb{F}^n$ para o qual (9) não admite nenhuma solução.

E10 Considere a seguinte sessão interativa de Python:

```
$ python
Python 3.9.13 (main, May 21 2022, 10:37:33)
[Clang 13.0.0 (clang-1300.0.29.30)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> D = {'A', 'B', 'C', 'D'}
>>> from vec import Vec
>>> a = Vec(D, {'B': 1, 'D': 5})
>>> b = Vec(D, {'A': -2, 'B': 1, 'C': 4, 'D': .5})
>>> c = Vec(D, {'B': 2})
>>> d = Vec(D, {'A': 2, 'B': 3, 'D':3})
>>> from vecutil import list2vec
>>> from triangular import triangular_solve
```

Queremos agora executar o comando

```
>>> x = triangular_solve([X, X, X, X], [Y, Y, Y, Y], list2vec([Z, Z, Z, Z]))
```

para resolver o sistema de 4 equações lineares

$$\begin{cases} \mathbf{a} \cdot \mathbf{x} = 3 \\ \mathbf{b} \cdot \mathbf{x} = 6 \\ \mathbf{c} \cdot \mathbf{x} = -8 \\ \mathbf{d} \cdot \mathbf{x} = -4. \end{cases}$$

Neste exercício, você deve dizer o que devem ser as listas `[X, X, X, X]`, `[Y, Y, Y, Y]` e `[Z, Z, Z, Z]` na chamada de `triangular_solve()` acima. Diga brevemente como você chegou a sua resposta. [*Observação.* Não deixe de calcular $\mathbf{a} \cdot \mathbf{x}$, $\mathbf{b} \cdot \mathbf{x}$, $\dots$, para verificar que você encontrou $\mathbf{x}$ corretamente.] ***{Data de entrega*: 5/9/2024}**

E11 Suponha que executamos uma sessão interativa do Python idêntica à sessão do Exercício **E10**, exceto pelo fato de definirmos `d` da seguinte forma:

```
>>> d = Vec(D, {'A': 2, 'B': 3, 'C': -1, 'D':3})
```

Queremos novamente resolver o sistema linear do Exercício **E10** fazendo uma chamada do procedimento `triangular_solve()` da forma

```
>>> x = triangular_solve([X, X, X, X], [Y, Y, Y, Y], list2vec([Z, Z, Z, Z]))
```

Isso é possível fazer? Justifique sua resposta.

E12 (Em preparação)

E13 (*i*) Seja $A = (\alpha_{ij})_{0\le i<m,\,0\le j<n} \in \mathbb{F}^{m\times n}$ uma matriz $m\times n$ com entradas em $\mathbb{F}$ e seja $\boldsymbol{\beta} = (\beta_j)_{0\le j<n} \in \mathbb{F}^n$ um vetor coluna. Verifique que, para todo $0 \le i < m$, a i-ésima entrada de $A\boldsymbol{\beta}$ é $\boldsymbol{\alpha}_i \cdot \boldsymbol{\beta}$, onde $\boldsymbol{\alpha}_i$ é a i-ésima linha de A, isto é,

$$A = \begin{bmatrix} \boldsymbol{\alpha}_0 \\ \vdots \\ \boldsymbol{\alpha}_{m-1} \end{bmatrix}. \tag{10}$$

(*ii*) Seja $M = (m_{ij})_{0\le i<r,\,0\le j<m} \in \mathbb{F}^{r\times m}$ uma matriz $r \times m$ com entradas em $\mathbb{F}$ e seja $\boldsymbol{\alpha} = (\alpha_j)_{0\le j<m} \in \mathbb{F}^m$ um vetor coluna. Ademais, suponha que $\mathbf{v}_j$ $(0 \le j < m)$ sejam as colunas de M:

$$M = \Big[\mathbf{v}_0 \mid \cdots \mid \mathbf{v}_{m-1}\Big]. \tag{11}$$

Verifique que a combinação linear dos $\mathbf{v}_j$ com coeficientes α_j é simplesmente $M\boldsymbol{\alpha}$, isto é,

$$\sum_{0\le j<m} \alpha_j \mathbf{v}_j = M\boldsymbol{\alpha}. \tag{12}$$

E14 Sejam $\mathbf{v}_0,\dots,\mathbf{v}_{m-1} \in \mathbb{F}^r$ e $\mathbf{u}_0,\dots,\mathbf{u}_{n-1} \in \mathbb{F}^r$ vetores coluna. Suponha que, para todo $0 \le j < n$,

$$\mathbf{u}_j = \sum_{0\le i<m} \alpha_{ij}\mathbf{v}_i. \tag{13}$$

Seja $\mathbf{w} = \sum_{0\le j<n} \beta_j \mathbf{u}_j$ uma combinação dos $\mathbf{u}_j$. Prove que $\mathbf{w}$ é uma combinação linear dos $\mathbf{v}_i$; mais precisamente, prove que $\mathbf{w} = \sum_{0\le i<m} \gamma_i \mathbf{v}_i$, onde, para todo $0 \le i < m$,

$$\gamma_i = \boldsymbol{\alpha}_i \cdot \boldsymbol{\beta}, \tag{14}$$

onde $\boldsymbol{\alpha}_i$ é o vetor linha $(\alpha_{ij})_{0\le j<n}$ e $\boldsymbol{\beta}$ é o vetor coluna $(\beta_i)_{0\le i<n}$. [*Sugestão.* Considere a matriz $A = (\alpha_{ij})_{0\le i<m,\,0\le j<n}$ e use **E13**.] **{*Data de entrega*: 5/9/2024}**

E15 (*M*) Leia a definição (abstrata) de espaços vetoriais na Wikipedia. Considere o conjunto dos números reais $\mathbb{R}$, com as operações usuais de soma e produto. Verifique que $\mathbb{R}$ é então um espaço vetorial sobre o corpo dos números racionais $\mathbb{Q}$.

E16 Faça o Problema 3.8.3 de **PNK**. Note que, com os vetores 011 e 101 de entrada, sua função deve devolver uma lista com os 4 elementos 000, 011, 101 e 110 (a ordem pode ser qualquer). Ademais, com a lista vazia de entrada, sua função deve devolver a lista contendo somente o vetor nulo de $\mathrm{GF}(2)^D$. [*Observação.* O enunciado do Problema 3.8.3 de **PNK** não deixa claro se a lista da saída pode ou não ter elementos repetidos. Em sua solução, você deve garantir que não haja elementos repetido em sua saída.] **{*Data de entrega*: 19/9/2024}**

E17 Faça os Problemas 3.8.7 a 3.8.10 de **PNK** (são quatro problemas). Lembre que um espaço vetorial é um conjunto de vetores que satisfaz as Propriedades V1, V2 e V3 (veja a Definição 3.4.1 em **PNK**).

E18 Seja D um conjunto arbitrário.

(i) Sejam U e $V \subset \mathbb{F}^D$ dois espaços vetoriais. Prove que $U \cap V$ é um espaço vetorial.

(ii) Seja dado $S \subset \mathbb{F}^D$. Prove que existe um "menor" espaço vetorial que contém S, isto é, um espaço vetorial $W \subset \mathbb{F}^D$ tal que (a) $S \subset W$ e que (b) se $S \subset V \subset \mathbb{F}^D$ e V é um espaço vetorial, então $W \subset V$. Note que um W que satisfaz (a) e (b) é único (isto é, tal "menor" espaço vetorial que contém S é único). [*Sugestão.* Para obter W, considere a interseção de todos os subespaços vetoriais de $\mathbb{F}^D$ que contêm S.]

E19 (M) Continuamos aqui o Exercício **E18**.

(i) Lembre que, dados vetores $\mathbf{v}_i \in \mathbb{F}^D$ $(1 \le i \le n)$, o espaço gerado por estes n vetores é

$$\operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \left\{ \sum_{1 \le i \le n} \alpha_i \mathbf{v}_i \colon \alpha_i \in \mathbb{F} \text{ para todo } i \right\}. \tag{15}$$

Seja S como no item (ii) do Exercício **E18**, e note que S pode ser um conjunto infinito. Colocamos

$$\operatorname{Span} S = \bigcup_T \operatorname{Span} T, \tag{16}$$

onde a união é sobre todo subconjunto finito T de S (se $T = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ $(n \ge 0)$, o conjunto $\operatorname{Span} T$ é dado por (15)). Prove que $\operatorname{Span} S$ definido em (16) é um espaço vetorial e que $S \subset \operatorname{Span} S$.

(ii) Prove que $\operatorname{Span} S$ definido em (16) é o menor espaço vetorial que contém S.

(iii) Suponha agora que $D = \mathbb{N} = \{0, 1, \dots\}$ e, para todo $n \in \mathbb{N}$, seja $e_n \in \mathbb{F}^D$ a função tal que $e_n(m) = 1$ se $m = n$ e $e_n(m) = 0$ se $m \ne n$. Seja $S = \{e_n \colon n \in \mathbb{N}\}$. Descreva os elementos de $\operatorname{Span} S$. É verdade que $\operatorname{Span} S = \mathbb{F}^D$?

E20 Seja D um conjunto arbitrário e seja $\emptyset \ne S \subset \mathbb{F}^D$. Prove que existe um "menor" espaço afim $A \subset \mathbb{F}^D$ que contém S.

E21 Neste exercício, suponha $\mathbb{F} = \mathbb{R}$ ou $\mathbb{F} = \mathbb{C}$. Seja D um conjunto arbitrário e seja $K \subset \mathbb{F}^D$. Dizemos que K é *convexo* se para quaisquer $\mathbf{x}$ e $\mathbf{y} \in K$, qualquer combinação convexa de $\mathbf{x}$ e $\mathbf{y}$ pertence a K (isto é, para quaisquer α e $\beta \ge 0$ tais que $\alpha + \beta = 1$, temos que $\alpha\mathbf{x} + \beta\mathbf{y} \in K$). Seja $S \subset \mathbb{F}^D$. Prove que existe um "menor" conjunto convexo $K \subset \mathbb{F}^D$ que contém S.

E22 Faça o Problema 4.17.12 de **PNK**.

E23 Um *grafo* G é um par ordenado (V, E), onde

$$E \subset \binom{V}{2} = \{e \subset V \colon |e| = 2\}. \tag{17}$$

Isto é, os elementos de E são da forma $\{x, y\}$ com x e y elementos distintos de V. Os elementos de V são os *vértices* de G e os de E são as *arestas* de G. Se $e = \{x, y\}$ é uma aresta, então e tem *extremos* ou *pontas* x e y e e *liga* x a y. Você pode ler um pouco sobre grafos na Wikipedia. O grafo ilustrado na primeira figura naquela página da Wikipedia é o grafo (V, E) com $V = \{1, \dots, 6\}$ e

$$E = \big\{\{1,2\}, \{2,3\}, \{3,4\}, \{4,5\}, \{5,1\}, \{2,5\}, \{4,6\}\big\}. \tag{18}$$

Para grafos pequenos, é usual especificar um desenho do grafo em vez dos conjuntos V e E, pois o desenho é mais simples de se entender. Desenhe todos os grafos com conjunto de vértices $V = \{1, 2, 3\}$ (são 8 grafos no total).

E24 (Continuação de **E23**) Às vezes, é útil permitir "arestas múltiplas" ou "arestas paralelas" em grafos: isto é, queremos mais de uma aresta ligando um par de vértices. Às vezes, é também útil permitir arestas que ligam um vértice a si próprio (tais arestas são chamadas de *laços*). Em tais contextos, trabalhamos com "multigrafos". Um *multigrafo* G é uma tripla (V, E, φ), onde V e E são conjuntos e $\varphi\colon E \to \binom{V}{2} \cup V$ é o que chamamos de *função de incidência* de G. Se $\varphi(e) = \{x, y\} \in \binom{V}{2}$, então a aresta e tem *extremos* x e y e ela *liga* x a y em G. Se $\varphi(e) = x \in V$, então a aresta e é um *laço*, que *liga* o vértice x consigo próprio. O multigrafo na Seção 4.11.2 de **PNK** (veja o segundo desenho desse multigrafo, em que as arestas estão rotuladas) é o multigrafo (V, E, φ), onde $V = \{1, 2, 3, 4\}$, $E = \{a, b, c, d, e\}$ e $\varphi(a) = \{1, 2\}$, $\varphi(b) = \varphi(c) = \{2, 3\}$, $\varphi(d) = \{1, 4\}$ e $\varphi(e) = \{2, 4\}$.

(i) No multigrafo da Seção 4.11.2 de **PNK**, quantos passeios há do vértice 3 para o vértice 2 de comprimento 4? E de comprimento 32? (Como você pode ler naquela seção, há 12 deles de comprimento 3.)

(ii) No grafo do Exercício **E23** (com conjunto de arestas (18)), quantos passeios há do vértice 1 ao vértice 6 de comprimento 32?

Em ambos os casos, diga como você chegou às respostas. **{*Data de entrega*: 19/9/2024}**

E25 Leia sobre *Lights Out* nesta página. Você pode jogar a versão 5×5 do Lights Out, por exemplo, nesta página. Leia agora o Exemplo 4.5.12 de **PNK**. Em particular, experimente executar o procedimento `button_vectors()` para valores pequenos de n para conferir que os vetores gerados correspondem realmente aos botões do jogo (o melhor é criar `B` com `coldict2mat()` e então fazer `print(B)`). Use o procedimento que você escreveu no Exercício **E16** para decidir se todas as configurações iniciais têm solução para $n = 2$, 3 e 4. Explique como você chegou a suas respostas.

E26 Leia o Exemplo 4.5.16 de **PNK**. Note que, para o uso de `solve` do módulo `solver.py`, você terá de usar Python 3.x com $x \in \{4, 5, 6\}$. Visite esta página e resolva a instância de Lights Out dada por ela usando o procedimento dado no Exemplo 4.5.16.

E27 (Continuação de **E26**) O Exemplo 4.5.16 de **PNK** descreve como resolver o Lights Out em uma sessão interativa do Python. Naturalmente, você pode escrever um programa para automatizar o processo. Escreva um programa Python, chamado `lo_solver.py`, que segue as seguintes especificações:

▷ *Entrada*: um inteiro N na linha de comando e pares de inteiros na entrada padrão especificando quais lâmpadas de uma instância $N \times N$ do Lights Out estão acesas.

▷ *Saída* (na saída padrão): pares de inteiros especificando quais botões devem ser pressionados para se resolver a instância dada.

Seu programa deve comportar-se necessariamente como você vê neste diretório. **{*Data de entrega*: 26/9/2024}**

E28 (Continuação de **E26**) Se você fosse pôr no ar uma página como essa, não seria muito bom se você permitisse que a página gerasse instâncias que não admitem solução. Diga como você pode gerar instâncias que sempre têm solução, usando a rotina `button_vectors()` do Exemplo 4.5.12 de **PNK**.

E29 Seja $G = (V, E)$ um grafo (veja **E23**). Dizemos que $F \subset E$ é um *ciclo* se todo vértice x de G é ponta de um número par de arestas em F, isto é, há um número par de $e \in F$ tal que $x \in e$. O *espaço de ciclos* de G é

$$\mathcal{C} = \{F \subset E \colon F \text{ é um ciclo em } G\}. \tag{19}$$

Seja M a *matriz de incidência* de G: a matriz em $\mathrm{GF}(2)^{V\times E}$ que tem como sua e-ésima coluna ($e \in E$) a função característica $\mathbb{1}_e \in \mathrm{GF}(2)^V$ de e (veja o Exercício **E3**). Prove que $\mathcal{C} = \{F \subset E \colon \mathbb{1}_F \in \operatorname{Null} M\}$.

E30 Seja $G = (E, V)$ um grafo e $\mathcal{C}$ o espaço dos ciclos de G. Prove que

$$\mathcal{C}' = \{\mathbb{1}_F \in \mathrm{GF}(2)^E \colon F \in \mathcal{C}\} \tag{20}$$

é um espaço vetorial sobre $\mathrm{GF}(2)$. [*Observação.* Para simplificar a notação, em geral identificamos $\mathcal{C}'$ com $\mathcal{C}$, identificando a função indicadora $\mathbb{1}_F$ com F.]

E31 Seja $G = (V, E)$ um grafo e seja $M \in \mathrm{GF}(2)^{V\times E}$ sua matriz de incidência (veja **E29**). Caracterize os grafos G tais que $\operatorname{Null} M = \{\mathbf{0}\}$. Prove que sua caracterização está correta. [*Sugestão.* Um *circuito* em um grafo é uma sequência de vértices e arestas

$$v_0, e_1, v_1, \dots, e_\ell, v_\ell \tag{21}$$

do grafo com $\ell > 0$ e tal que (a) $e_i = \{v_{i-1}, v_i\}$ para todo $1 \le i \le \ell$, (b) os vértices $v_0, v_1, \dots, v_{\ell-1}$ são todos distintos e (c) $v_\ell = v_0$. O que ocorre se G contém um circuito?]

E32 Seja $G = (V, E)$ um grafo e $F \subset E$ um ciclo de G (veja Exercício **E29**).

(i) Prove que existem circuitos $C_1, \dots, C_t$ ($t \ge 0$) tais que

- (a) os C_i ($1 \le i \le t$) dois a dois não têm arestas em comum e
- (b) $F = E(C_1) \cup \dots \cup E(C_t)$, onde $E(C_i)$ denota o conjunto de arestas que ocorrem em C_i.

(ii) Conclua que $\mathbb{1}_F = \sum_{1\le i\le t} \mathbb{1}_{C_i}$.

E33 Seja $G = (V, E)$ um grafo. Assim como no Exercício **E29**, trabalhamos neste exercício sobre $\mathrm{GF}(2)$. O *espaço dos cociclos* de G é

$$\mathcal{C}^\perp = \{B \subset E \colon \mathbb{1}_B^\top \mathbb{1}_C = 0 \text{ para todo ciclo } C \text{ de } G\}. \tag{22}$$

Os elementos de $\mathcal{C}^\perp$ são os *cociclos* de G.

(i) Prove que $\mathcal{C}^\perp$ é um subespaço vetorial de $\mathrm{GF}(2)^E$. [*Observação.* Como no Exercício **E30**, aqui identificamos $B \subset E$ com $\mathbb{1}_B \in \mathrm{GF}(2)^E$.]

(ii) Para todo $U \subset V$, seja

$$B_U = \{e \in E \colon e \text{ tem uma ponta em } U \text{ e a outra ponta em } V \setminus U\}. \tag{23}$$

Prove que B_U é um cociclo de G para qualquer $U \subset V$. [*Observação.* O conjunto B_U é o assim chamado *corte* definido por U.]

(iii) Sejam dados U e $W \subset V$. Prove que

$$B_U \bigtriangleup B_W = B_{U \bigtriangleup W}, \tag{24}$$

onde $\bigtriangleup$ denota a diferença simétrica.

(iv) Prove que

$$\mathcal{B} = \{B_U \colon U \subset V\} \tag{25}$$

é um subespaço vetorial de $\mathcal{C}^\perp$, onde estamos identificando aqui $B_U \subset E$ com $\mathbb{1}_{B_U} \in \mathrm{GF}(2)^E$.

E34 Um grafo $G = (V, E)$ é uma *árvore* se G é uma floresta (isto é, não contém circuitos) e é conexo (isto é, existe caminho de x a y para qualquer par de vértices x e $y \in V$). Seja G uma árvore com $n \geq 1$ vértices.

(i) Prove que G tem $n - 1$ arestas.

(ii) Determine $\mathcal{C}^\perp$ e $\mathcal{B}$ definidos em (22) e (25) para G.

(iii) Seja $F \subset E$ um conjunto qualquer de arestas de G. Prove que $F = B_U$ para algum $U \subset V$. [*Observação.* Esse fato pode ser provado diretamente, com um argumento envolvendo grafos, ou pode ser derivado imediatamente de (ii) acima.]

{*Data de entrega*: 6/10/2024}

E35 Seja $G = (V, E)$ um grafo. Neste exercício, vamos dizer que $F \subset E$ é *ímpar-regular em* G se todo vértice x de G é ponta de um número ímpar de arestas em F, isto é, há um número ímpar de $e \in F$ tal que $x \in e$.

(i) Suponha que G seja o grafo exemplo na página da Wikipedia, com conjunto de arestas (18). Encontre um conjunto ímpar-regular de arestas em G.

(ii) Seja $M \in \mathrm{GF}(2)^{V \times E}$ a matriz de incidência de um grafo G. Prove que $F \subset E$ é ímpar-regular em G se e só se $M\mathbb{1}_F = \mathbb{1}_V$.

(iii) Suponha agora que G seja um grafo com número ímpar de vértices. Prove que G não admite um conjunto ímpar-regular de arestas (isto é, não existe $F \subset E$ ímpar-regular em G). [*Sugestão.* Multiplique os dois lados de $M\mathbb{1}_F = \mathbb{1}_V$ por $\mathbb{1}_V^\top$ pela esquerda. Não se esqueça que estamos trabalhando sobre $\mathrm{GF}(2)$].

E36 Sejam R e C conjuntos finitos e $\mathbb{F}$ um corpo. Seja $\mathbb{F}^{R \times C}$ o conjunto das matrizes $R \times C$ e $L(\mathbb{F}^C, \mathbb{F}^R)$ o conjunto das funções lineares de $\mathbb{F}^C$ para $\mathbb{F}^R$. Dado $A \in \mathbb{F}^{R \times C}$, definimos $f_A \in L(\mathbb{F}^C, \mathbb{F}^R)$ pondo $f_A(\mathbf{x}) = A\mathbf{x}$ para todo $\mathbf{x} \in \mathbb{F}^C$. Ademais, dado $f \in L(\mathbb{F}^C, \mathbb{F}^R)$, construímos a matriz A_f que tem como sua c-ésima coluna o vetor $f(\mathbf{e}_c) \in \mathbb{F}^R$ para todo $c \in C$, onde $\mathbf{e}_c \in \mathbb{F}^R$ é a função característica $\mathbb{1}_{\{e\}}$ do conjunto $\{c\} \subset C$. Prove que estas duas operações são inversas uma da outra, isto é, prove as seguintes duas afirmações:

(i) Para todo $A \in \mathbb{F}^{R \times C}$, vale que $A_{f_A} = A$.

(ii) Para todo $f \in L(\mathbb{F}^C, \mathbb{F}^R)$, vale que $f_{A_f} = f$.

E37 Sejam dados $f \in F(\mathbb{F}^R, \mathbb{F}^S)$ e $g \in L(\mathbb{F}^S, \mathbb{F}^T)$.

(i) Prove que $g \circ f \in F(\mathbb{F}^R, \mathbb{F}^T)$.

(ii) Sejam A_f, A_g e $A_{g \circ f}$ como definidos no Exercício **E36**. Prove que $A_{g \circ f} = A_g A_f$.

E38 Sejam $h\colon X \to Y$ e $g\colon Y \to X$ duas funções. Sejam $\mathrm{id}_X\colon X \to X$ e $\mathrm{id}_Y\colon Y \to Y$ as funções identidades sobre X e Y. Suponha que $h \circ g = \mathrm{id}_Y$. É verdade que necessariamente $g \circ h = \mathrm{id}_X$? Prove ou dê um contra-exemplo.

E39 Sejam X e Y dois conjuntos finitos de mesma cardinalidade.

(i) Suponha que $f\colon X \to Y$ seja uma função injetora. Prove que f é sobrejetora.

(ii) Suponha que $f\colon X \to Y$ seja uma função sobrejetora. Prove que f é injetora.

E40 Sejam X e Y dois conjuntos finitos de mesma cardinalidade, e sejam $h\colon X \to Y$ e $g\colon Y \to X$ duas funções tais que $h \circ g = \mathrm{id}_Y$. Prove que $g \circ h = \mathrm{id}_X$. **{*Data de entrega*: 6/10/2024}**

E41 Sejam U e V espaços vetoriais sobre $\mathbb{F}$ e seja $f\colon U \to V$ uma função linear. Suponha que f seja inversível e seja $g = f^{-1}\colon V \to U$ sua inversa. Prove que g é uma função linear.

E42 Prove ou dê contraexemplos:

(*i*) Sejam $g\colon X \to Y$ e $f\colon Y \to Z$ funções tais que $f \circ g$ é inversível. Então tanto f quanto g são inversíveis.

(*ii*) Sejam $A \in \mathbb{F}^{R\times C}$ e $B \in \mathbb{F}^{C\times D}$ matrizes tais que o produto $AB \in \mathbb{F}^{R\times D}$ é inversível. Então tanto A quanto B são inversíveis.

(*iii*) Sejam $A \in \mathbb{F}^{R\times C}$ e $B \in \mathbb{F}^{C\times R}$ matrizes. Sejam I_R a matriz identidade em $\mathbb{F}^{R\times R}$ e I_C a matriz identidade em $\mathbb{F}^{C\times C}$. Se $AB = I_R$, então A é inversível e $A^{-1} = B$.

(*iv*) Sejam A, B, I_R e I_C como em (*iii*) acima. Se $AB = I_R$, então B é inversível e $B^{-1} = A$.

E43 Leia a Seção 4.14 de **PNK** (partes iniciais). Lembre que o código de Hamming que vimos em sala é, por definição, o conjunto $\operatorname{Null} H = \operatorname{Ker} f_H$, onde

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{26}$$

e $f_H\colon \mathrm{GF}(2)^7 \to \mathrm{GF}(2)^3$ é função que leva $\mathbf{v} \in \mathrm{GF}(2)^7$ em $H\mathbf{v} \in \mathrm{GF}(2)^3$ (veja Seção 4.7.5 de **PNK**). Seja G a matriz dada na Seção 4.14.3 de **PNK**. Sejam $G_{*1}, \dots, G_{*4}$ as quatro colunas de G, de forma que $G = [G_{*1} \mid \cdots \mid G_{*4}]$. O espaço das colunas de G é, por definição, $\operatorname{Span}\{G_{*1}, \dots, G_{*4}\} \subset \mathrm{GF}(2)^7$. Prove que o espaço das colunas de G coincide com o código de Hamming, isto é, prove que

$$\operatorname{Null} H = \operatorname{Span}\{G_{*1}, \dots, G_{*4}\}. \tag{27}$$

[*Sugestão.* É fácil verificar que $\operatorname{Null} H \supset \operatorname{Span}\{G_{*1}, \dots, G_{*4}\}$. Para verificar a outra direção, considere um elemento $[c_1 \cdots c_7]^\top \in \operatorname{Null} H$. Considere $G\mathbf{w}$, onde $\mathbf{w} = [c_7\ c_6\ c_5\ c_3]^\top$. O Exercício **E45** mostra como podemos obter a matriz G a partir de H de forma sistemática.]

E44 Verifique os seguintes fatos.

(*i*) Seja $A \in \mathbb{F}^{R\times C}$ uma matriz e $\{C_1, C_2\}$ uma partição de C, isto é, $C = C_1 \cup C_2$, $C_1 \cap C_2 = \emptyset$ e $C_1 \neq \emptyset$ e $C_2 \neq \emptyset$. Sejam $A_1 \in \mathbb{F}^{R\times C_1}$ e $A_2 \in \mathbb{F}^{R\times C_2}$ as matrizes naturalmente definidas por A por restrição (por exemplo, $A_1(r,c) = A(r,c)$ para todo $(r,c) \in R \times C_1$). Seja $\mathbf{v} \in \mathbb{F}^C$ e defina $\mathbf{v}_1 \in \mathbb{F}^{C_1}$ e $\mathbf{v}_2 \in \mathbb{F}^{C_2}$ de forma análoga. Prove que $A\mathbf{v} = A_1\mathbf{v}_1 + A_2\mathbf{v}_2$. Uma forma intuitiva de se entender esse fato é escrever algo como

$$A\mathbf{v} = \begin{bmatrix} A_1 \,|\, A_2 \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 \\ \hline \mathbf{v}_2 \end{bmatrix} = A_1\mathbf{v}_1 + A_2\mathbf{v}_2 \tag{28}$$

ou simplesmente

$$A\mathbf{v} = \begin{bmatrix} A_1 & A_2 \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} = A_1\mathbf{v}_1 + A_2\mathbf{v}_2 \tag{29}$$

(*ii*) Sejam A, $\mathbf{v}$, C_1 e C_2, A_1 e A_2 e $\mathbf{v}_1$ e $\mathbf{v}_2$ como acima. Suponha agora que $\{R_1, R_2\}$ seja uma partição de R. Sejam $A_{ij} \in \mathbb{F}^{R_i \times C_j}$ para todo i e j definidos por restrição de A. Prove que $A\mathbf{v} = \mathbf{u}_1 \cup \mathbf{u}_2$, onde $\mathbf{u}_1 = A_{11}\mathbf{v}_1 + A_{12}\mathbf{v}_2$, $\mathbf{u}_2 = A_{21}\mathbf{v}_1 + A_{22}\mathbf{v}_2$ e você precisa encontrar a interpretação correta para a união $\mathbf{u}_1 \cup \mathbf{u}_2$. Uma forma intuitiva de se entender esse fato é escrever algo como

$$A\mathbf{v} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} A_{11}\mathbf{v}_1 + A_{12}\mathbf{v}_2 \\ A_{21}\mathbf{v}_1 + A_{22}\mathbf{v}_2 \end{bmatrix}. \tag{30}$$

(iii) Nos itens anteriores, podemos substituir $\mathbf{v}$ por uma matriz $B \in \mathbb{F}^{C \times D}$ e considerar uma partição $\{D_1, D_2\}$ de D. Interprete adequadamente e verifique a identidade

$$AB = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{bmatrix}. \tag{31}$$

E45 Como de usual, sejam R e C conjuntos de índices que indexam as linhas e colunas de matrizes. Suponha que $R \subset C$ e seja $C' = C \setminus R$ de forma que $C = R \cup C'$. Seja $H \in \mathbb{F}^{R \times C}$ com o seguinte formato especial: $H_1 \in \mathbb{F}^{R \times R}$ obtido por restrição de H é a matriz identidade $I_R \in \mathbb{F}^{R \times R}$. Intuitivamente,

$$H = \begin{bmatrix} I_R \ M \end{bmatrix} \tag{32}$$

onde M é uma matriz em $\mathbb{F}^{R \times C'} = \mathbb{F}^{R \times (C \setminus R)}$. Seja

$$G = \begin{bmatrix} -M \\ I_{C'} \end{bmatrix} \in \mathbb{F}^{C \times C'}, \tag{33}$$

onde $I_{C'} \in \mathbb{F}^{C' \times C'}$ é a matriz identidade.

(i) Calcule HG.

(ii) Prove que

$$\operatorname{Null} H = \operatorname{Span}\{G_{*c} \colon c \in C'\}, \tag{34}$$

onde $G_{*c} \in \mathbb{F}^C$ é a c-ésima coluna de G para todo $c \in C'$.

(iii) Seja

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathrm{GF}(2)^{4 \times 15} \tag{35}$$

Encontre uma matriz G tal que $\operatorname{Null} H$ é o espaço gerado pelas colunas de G. [*Observação.* Tal matriz G é meio grande, mas ela não é muito densa e com um pouco de paciência você consegue escrevê-la explicitamente.]

{*Data de entrega*: 13/10/2024}

E46 Sejam $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{F}^m$ vetores e seja $M = [\mathbf{v}_1 \mid \cdots \mid \mathbf{v}_n] \in \mathbb{F}^{m \times n}$ a matriz cujas colunas são os $\mathbf{v}_i$. Suponha que exista uma matriz $N \in \mathbb{F}^{n \times m}$ tal que $NM = I_n$, onde $I_n \in \mathbb{F}^{n \times n}$ é a matriz identidade $n \times n$. Prove que os $\mathbf{v}_i$ $(1 \le i \le n)$ são linearmente independentes.

E47 Seja $G = (V, E)$ um grafo. Para cada $e \in E$, seja $\mathbb{1}_e \in \mathrm{GF}(2)^V$ a função característica de e.

(i) Seja

$$\mathbf{d} = \sum_{e \in E} \mathbb{1}_e. \tag{36}$$

Verifique que $\mathbf{d} \in \mathrm{GF}(2)^V$ é tal que $\mathbf{d}(v) = 1$ se e só se v tem grau ímpar em G (o *grau* de um vértice é o número de arestas que contém aquele vértice).

(*ii*) Seja $\mathbf{j}_V \in \mathrm{GF}(2)^V$ tal que $\mathbf{j}_V(v) = 1$ para todo $v \in V$. Prove que

$$\mathbf{j}_V^\top \sum_{e \in E} \mathbb{1}_e = 0, \tag{37}$$

lembrando que estamos trabalhando em $\mathrm{GF}(2)$.

(*iii*) Deduza que G tem um número par de vértices de grau ímpar. [*Observação.* Note que este fato generaliza o Exercício **E35**(*iii*).]

E48 Seja $G = (V, E)$ um grafo e sejam x e y dois vértices em G. Seja $F \subset E$ um subconjunto de arestas de G. Suponha que

$$\sum_{f \in F} \mathbb{1}_f = \mathbb{1}_{\{x,y\}}, \tag{38}$$

onde estamos trabalhando em $\mathrm{GF}(2)$. Isto é, as funções características $\mathbb{1}_f \in \mathrm{GF}(2)^V$ das arestas f em F somam a função característica $\mathbb{1}_{\{x,y\}} \in \mathrm{GF}(2)^V$ de $\{x, y\}$.

(*i*) Verifique que (38) é equivalente a dizer que $M\mathbb{1}_F = \mathbb{1}_{\{x,y\}}$, onde M é a matriz de incidência de G (veja o Exercício **E29**).

(*ii*) É verdade que (38) implica que F é o conjunto de arestas de um (x, y)-caminho em G? Lembre que um (x, y)-*caminho* é um caminho que começa em x e termina em y.

(*iii*) Considere o grafo $H = (V, F)$, que tem o mesmo conjunto de vértices que G, mas tem como conjunto de arestas o conjunto F. Prove que (38) implica que existe um (x, y)-caminho em H. [*Sugestão.* Considere o conjunto $A \subset V$ dos vértices acessíveis a partir do vértice x no grafo H. Seja $B = V \setminus A$. Verifique que toda aresta $f \in F$ é tal que ou suas duas pontas estão em A ou suas duas pontas estão em B. Seja $F_A \subset F$ o conjunto das arestas em F que têm suas duas pontas em A e seja $F_B = F \setminus F_A$. Considere o grafo $J = (A, F_A)$. O que (38) diz sobre J? (Tenha em mente o Exercício **E47**).]

E49 Seja $G = (V, E)$ um grafo. Dizemos que $F \subset E$ é *aresta-gerador* se para toda aresta $\{x, y\} \in E$, existe um (x, y)-caminho em G que usa somente arestas em F. Considere as funções características $\mathbb{1}_e \in \mathrm{GF}(2)^V$ $(e \in E)$ das arestas de G. Prove que $F \subset E$ é aresta-gerador se e só se

$$\mathrm{Span}\{\mathbb{1}_f : f \in F\} = \mathrm{Span}\{\mathbb{1}_e : e \in E\}. \tag{39}$$

[*Observação.* O espaço no lado direito de (39) é às vezes conhecido como o *espaço das arestas de G* e é denotado $C_1(G)$]

E50 Fixe um inteiro $n \geq 3$ e seja $R = \{1, \ldots, n\}$. Para todo $1 \leq i < n$, seja $\mathbf{f}_i = \mathbb{1}_{\{i,i+1\}}$, e seja $\mathbf{f}_n = \mathbb{1}_{\{1,n\}}$ (isto é, estamos considerando as funções características dos conjuntos $\{1, 2\}$, $\{2, 3\}$, ..., $\{n - 1, n\}$ e $\{n, 1\}$).

(*i*) Suponha que estamos trabalhando sobre $\mathrm{GF}(2)$. Mostre que os vetores $\mathbf{f}_i$ $(1 \leq i \leq n)$ são linearmente dependentes sobre $\mathrm{GF}(2)$.

(*ii*) Suponha agora que n seja par e que estamos agora trabalhando sobre os números reais $\mathbb{R}$. Mostre que os vetores $\mathbf{f}_i$ $(1 \leq i \leq n)$ são linearmente dependentes sobre $\mathbb{R}$.

(*iii*) Suponha agora que n seja ímpar. Mostre que os vetores $\mathbf{f}_i$ $(1 \leq i \leq n)$ são linearmente independentes sobre $\mathbb{R}$. [*Sugestão.* Observe, por exemplo, que

$$\begin{bmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = 2I_3 \tag{40}$$

e

$$\begin{bmatrix} 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} = 2I_5. \tag{41}$$

Generalize e use o resultado do Exercício **E46**.]

***{Data de entrega*: 13/10/2024}**

E51 (M) Lembre que $\mathbb{R}$ é um espaço vetorial sobre $\mathbb{Q}$ (veja o Exercício **E15**).

(*i*) Prove que 1 e $\sqrt{2}$ são linearmente independentes sobre $\mathbb{Q}$.

(*ii*) Prove que $\sqrt{2}$ e $\sqrt{3}$ são linearmente independentes sobre $\mathbb{Q}$. Generalize (você pode considerar valores diferentes de 2 e 3 e pode também considerar mais de dois valores).

E52 Note que $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{R}$ de forma natural (isto é semelhante ao fato que $\mathbb{R}$ é um espaço vetorial sobre $\mathbb{Q}$; veja o Exercício **E15**). Encontre dois vetores em $\mathbb{C}$ que são linearmente independentes sobre $\mathbb{R}$, mas que são linearmente dependentes sobre $\mathbb{C}$.

E53 Sejam $\mathbf{v}_1, \ldots, \mathbf{v}_n$ vetores em $\mathbb{R}^N$ que são linearmente independentes em $\mathbb{R}^N$. Naturalmente, podemos também considerar $\mathbf{v}_1, \ldots, \mathbf{v}_n$ como vetores em $\mathbb{C}^N$. Prove que eles também são linearmente independentes em $\mathbb{C}^N$.

E54 Senhor Cético não acredita que *Lights Out* no tabuleiro 20×20 *sempre* tem solução. Como você pode convencê-lo desse fato? Sr. C está disposto a verificar soluções de instâncias específicas de *Lights Out* (ele tem um programa que verifica a correção de soluções apresentadas a ele), mas não está disposto a procurar soluções. Por outro lado, Sr. C tem acesso a um gerador de bits aleatórios e ele acredita que eventos com probabilidade menor ou igual a $1/2^{70} \approx 10^{-21}$ não acontecem (a idade do universo é algo como 5×10^{17} segundos). Use o fato que você resolveu o Exercício **E27**, e você pode usar seu programa `lo_solver.py`.

E55 Sejam V um espaço vetorial e S um subconjunto de V. Prove que as seguintes afirmações são equivalentes.

(*i*) S é uma base de V.

(*ii*) S é um conjunto gerador *minimal* de V, isto é, $\operatorname{Span} S = V$, mas, para todo $S' \subset S$ com $S' \neq S$, vale que $\operatorname{Span} S' \neq V$.

(*iii*) S é um conjunto linearmente independente *maximal* em V, isto é, S é linearmente independente, mas, para todo $S' \subset V$ com $S \subset S'$ e $S \neq S'$, vale que S' não é linearmente independente.

(*iv*) S é um conjunto gerador de V com a propriedade de *representação única*, isto é, $\operatorname{Span} S = V$ e, para todo $\mathbf{v} \in V$, existe uma única combinação linear de elementos de S que é igual a $\mathbf{v}$.

***{Data de entrega*: 20/10/2024}**

E56 Lembre que um grafo G é *acíclico* se ele não contém circuitos e é *conexo* se, para quaisquer dois vértices x e y em G, há um (x, y)-caminho em G. Seja $G = (V, E)$ um grafo e considere

$$S = \{\mathbb{1}_e : e \in E\} \subset \mathrm{GF}(2)^V \tag{42}$$

e

$$W = \mathrm{Span}\{\mathbb{1}_{\{x,y\}} : x, y \in V \text{ e } x \neq y\} \subset \mathrm{GF}(2)^V. \tag{43}$$

(*i*) Prove que $\mathrm{Span}\, S = W$ se e só se G for conexo.

(*ii*) Prove que S é linearmente independente se e só se G for acíclico.

[*Sugestão.* Use o Exercício **E48**(*iii*).]

E57 Lembre que um grafo G é uma *árvore* se ele for *conexo* e *acíclico*. Prove que as seguintes asserções são equivalentes para um grafo $G = (V, E)$:

(*i*) G é uma árvore.

(*ii*) Os vetores $\mathbb{1}_e \in \mathrm{GF}(2)^V$ $(e \in E)$ formam um base do espaço

$$W = \mathrm{Span}\{\mathbb{1}_{\{x,y\}} : x, y \in V \text{ e } x \neq y\} \subset \mathrm{GF}(2)^V. \tag{44}$$

E58 Deduza dos Exercícios **E55**–**E57** que as seguintes asserções são equivalentes para um grafo $G = (V, E)$:

(*i*) G é uma árvore.

(*ii*) (Minimalmente conexo) G é conexo, e a remoção de qualquer aresta de G resulta em um grafo desconexo, isto é, $(V, E \setminus \{e\})$ é desconexo para qualquer $e \in E$.

(*iii*) (Maximalmente acíclico) G não contém circuitos, mas a adição de qualquer nova aresta $f \subset V$ a G resulta em um grafo que contém um circuito, isto é, $(V, E \cup \{f\})$ contém um circuito para qualquer $f \in \binom{V}{2} \setminus E$.

(*iv*) (Unicidade dos caminhos) Para quaisquer vértices x e y de G, existe um único (x, y)-caminho em G.

E59 Provamos em sala que o Algoritmo Grow encontra uma floresta de peso mínimo em um grafo com custo nas arestas. A prova dependeu de uma hipótese adicional, a saber, que os custos das arestas são todos distintos. Prove o resultado sem essa hipótese. [*Sugestão.* Ao escolher F^*, suponha adicionalmente que F^* e F tenham o maior número possível de arestas em comum, e repita o argumento.] **{*Data de entrega*: 20/10/2024}**

E60 Seja $2^{\mathbb{N}} = \mathcal{P}(\mathbb{N})$ o conjunto das partes de $\mathbb{N}$. Para cada uma das famílias $\mathcal{F} \subset 2^{\mathbb{N}}$ abaixo, diga se existe em $\mathcal{F}$ um elemento maximal em $\mathcal{F}$, isto é, um $F^* \in \mathcal{F}$ tal que se $F^* \subset F'$ e $F^* \neq F'$, então $F' \notin \mathcal{F}$. Justifique suas respostas.

(*i*) $\mathcal{F} = \{F \subset \mathbb{N} : \mathbb{N} \setminus F \text{ é um conjunto infinito}\}$

(*ii*) $\mathcal{F} = \{F \subset \mathbb{N} : F \text{ é tal que } n^{-1}|F \cap \{0, 1, \ldots, n-1\}| \leq 1/2 \text{ para todo } n > 0\}$

E61 Seja X um conjunto finito.

(*i*) Suponha que $\mathcal{F} \subset \mathcal{P}(X)$ seja uma família de subconjuntos de X tal que (*a*) $|F|$ é ímpar para todo $F \in \mathcal{F}$ e (*b*) $|F \cap F'|$ é par para quaisquer dois F e F' membros distintos de $\mathcal{F}$. Prove que $\mathcal{F}$ tem no máximo $|X|$ membros. [*Sugestão.* Considere as funções características $\mathbb{1}_F \in \mathrm{GF}(2)^X$ dos membros F de $\mathcal{F}$ e prove que eles são linearmente independentes (considere uma combinação linear deles, considere um $F_0 \in \mathcal{F}$ arbitrário, e multiplique a combinação linear por $\mathbb{1}_{F_0}$).]

(*ii*) Encontre uma família $\mathcal{F}$ como em (*i*) acima com $|\mathcal{F}| = |X|$.

(iii) Encontre uma família $\mathcal{F} \subset \mathcal{P}(X)$ tal que $|F \cap F'|$ é par para quaisquer dois F e F' membros de $\mathcal{F}$ com $|\mathcal{F}| \geq 2^{\lfloor |X|/2 \rfloor}$.

{*Data de entrega*: 3/11/2024}

E62 Seja p um primo e X um conjunto finito.

(i) Suponha que $\mathcal{F} \subset \mathcal{P}(X)$ seja uma família de subconjuntos de X tal que (a) $|F| \not\equiv 0 \pmod p$ para todo $F \in \mathcal{F}$ e (b) $|F \cap F'| \equiv 0 \pmod p$ para quaisquer dois F e F' membros distintos de $\mathcal{F}$. Prove que $\mathcal{F}$ tem no máximo $|X|$ membros.

(ii) Encontre uma família $\mathcal{F}$ como em (i) acima com $|\mathcal{F}| = |X|$.

(iii) Encontre uma família $\mathcal{F} \subset \mathcal{P}(X)$ tal que $|F \cap F'| \equiv 0 \pmod p$ para quaisquer dois F e F' membros de $\mathcal{F}$ com $|\mathcal{F}| \geq 2^{\lfloor |X|/p \rfloor}$.

E63 Sejam $A \in \mathbb{F}^{P \times Q}$ e $B \in \mathbb{F}^{R \times S}$ duas matrizes. Definimos a matriz $A \otimes B \in \mathbb{F}^{(P \times R) \times (Q \times S)}$ como a matriz com entradas

$$(A \otimes B)\big((p, r), (q, s)\big) = A(p, q)B(r, s) \tag{45}$$

para todo $\big((p, r), (q, s)\big) \in (P \times Q) \times (R \times S)$. Mais intuitivamente, suponha que

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}. \tag{46}$$

Então

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}. \tag{47}$$

Sejam agora $H_1, H_2, \dots$ matrizes com entradas em $\{-1, 1\}$ dadas por

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{48}$$

e, para todo $n \geq 2$,

$$H_n = H_1 \otimes H_{n-1}. \tag{49}$$

(i) Calcule H_2 e H_3.

(ii) Quantas linhas e quantas colunas tem H_n?

(iii) Calcule H_n^2 para todo n.

E64 Considere as matrizes H_n ($n \geq 1$) do Exercício **E63**. Sejam $\mathbf{v}_1, \dots, \mathbf{v}_N \in \{-1, 1\}^N$ as N colunas de H_n, de forma que

$$H_n = [\mathbf{v}_1 \mid \cdots \mid \mathbf{v}_N]. \tag{50}$$

Prove que os $\mathbf{v}_i$ ($1 \leq i \leq N$) formam uma base de $\mathbb{F}^N$ para $\mathbb{F} = \mathbb{R}$ e $\mathbb{F} = \mathbb{C}$, isto é, prove que eles geram $\mathbb{F}^N$ e que eles são linearmente independentes sobre $\mathbb{F}$. Esses vetores são uma base de $\mathrm{GF}(2)^N$?

E65 Responda e justifique:

(i) Qual é a dimensão do espaço vetorial das matrizes $\{M \colon M \in \mathbb{F}^{R \times C}\}$ sobre $\mathbb{F}$?

(ii) Qual é a dimensão do espaço vetorial das *matrizes simétricas*

$$\{M \colon M \in \mathbb{F}^{S \times S} \text{ tal que } M = M^\top\} \tag{51}$$

sobre $\mathbb{F}$?

(*iii*) Qual é a dimensão do espaço vetorial das *matrizes antissimétricas*

$$\{M\colon M \in \mathbb{F}^{S\times S} \text{ tal que } M = -M^\top\} \tag{52}$$

sobre $\mathbb{F}$?

E66 (M) Considere $\mathbb{R}$ como um espaço vetorial sobre $\mathbb{Q}$. Prove que a dimensão desse espaço é infinito. Prove que essa dimensão não é nem enumerável.

E67 (*i*) Prove que, para todo inteiro $n \geq 0$, temos

$$(1-x)\sum_{0\leq i<n} x^i = 1 - x^n. \tag{53}$$

(*ii*) Fixe $n \geq 1$ e seja $\omega = \mathrm{e}^{2\pi\mathbf{i}/n}$, onde $\mathbf{i} = \sqrt{-1}$. Seja $S = \{0, 1, \ldots, n-1\}$ e considere a matriz $F_n \in \mathbb{C}^{S\times S}$ tal que $F_n(i,j) = \omega^{ij}$ para todo i e j em S. Calcule F_2, F_3 e F_4 explicitamente.

(*iii*) Considere a matriz $G_n \in \mathbb{C}^{S\times S}$ tal que $G_n(i,j) = \omega^{-ij}$ para todo i e j em S. Calcule G_nF_n e F_nG_n para todo $n \geq 1$.

(*iv*) Sejam $\mathbf{v}_0, \ldots, \mathbf{v}_{n-1} \in \mathbb{C}^S$ as n colunas de F_n, de forma que

$$F_n = [\mathbf{v}_0 \mid \cdots \mid \mathbf{v}_{n-1}]. \tag{54}$$

Prove que os $\mathbf{v}_i$ $(0 \leq i < n)$ formam uma base de $\mathbb{C}^S$. Prove o mesmo para as colunas de G_n.

E68 Sejam V e W espaços vetoriais sobre $\mathbb{F}$. Seja $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ um conjunto de n vetores linearmente independentes de V e seja $\varphi\colon S \to W$ uma função qualquer.

(*i*) Prove que existe uma função linear $f\colon \operatorname{Span} S \to W$ tal que $f(\mathbf{v}_i) = \varphi(\mathbf{v}_i)$ para todo $1 \leq i \leq n$.

(*ii*) Prove que f como em (*i*) acima é única.

{*Data de entrega*: 3/11/2024}

E69 Seja $G = (V, E)$ um grafo conexo e seja $T = (V, F)$ com $F \subset E$ uma árvore (veja Exercício **E57**). Como G e T têm o mesmo conjunto de vértices, dizemos que T é uma *árvore geradora* de G (em teoria dos grafos, esse fato é expressado dizendo que T não só é um *subgrafo* de G, mas é um subgrafo *gerador* de G). Seja $A \subset E$ um conjunto acíclico de arestas de G (isto é, tal que (V, A) não contém um circuito). Mostre que existe $F' \subset F$ tal que $T' = (V, A \cup F')$ é uma árvore geradora de G. [*Sugestão.* Aplique o morphing lemma.]

E70 Seja S um conjunto de vetores de $\mathbb{F}^D$ com D finito. Definimos o *posto* de S como sendo $\dim \operatorname{Span} S$. Prove que o posto de S é

$$\max\{|T|\colon T \subset S \text{ com } T \text{ linearmente independente}\}. \tag{55}$$

E71 Suponha que sorteamos $\mathbf{a}_i \in \mathrm{GF}(2)^n$ uniformemente ao acaso para todo $1 \leq i \leq n$, independentemente. Prove que o valor esperado do posto da coleção de vetores $\mathbf{a}_1, \ldots, \mathbf{a}_n$ é maior que $n-1$. [*Sugestão.* Considere os eventos $E_i = \{\mathbf{a}_i \notin \operatorname{Span}\{\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}\}\}$ e note que $\operatorname{posto}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} = \sum_i \mathbb{1}_{E_i}$. Note que $\mathbb{E}(\mathbb{1}_{E_i}) = \mathbb{P}(E_i) \geq 1 - 2^{i-1-n}$.]

E72 Sejam U e W subespaços complementares em V, de forma que $V = U \oplus W$. Sabemos que, para todo $\mathbf{v} \in V$, existem $\mathbf{u} \in U$ e $\mathbf{w} \in W$ tais que $\mathbf{v} = \mathbf{u} + \mathbf{w}$ e que esses vetores $\mathbf{u}$

e $\mathbf{w}$ são únicos. Defina a função $f\colon V \to U$ pondo $f(\mathbf{v}) = \mathbf{u}$ para todo $\mathbf{v} \in V$, onde $\mathbf{u}$ é como acima. Prove que f é uma função linear.

E73 Sejam V e W espaços vetoriais, $f\colon V \to W$ uma função linear, e $\mathbf{b}_1, \dots, \mathbf{b}_n \in V$ elementos de V.

(i) Suponha que f seja injetor e que $\mathbf{b}_1, \dots, \mathbf{b}_n$ sejam linearmente independentes. Prove que $f(\mathbf{b}_1), \dots, f(\mathbf{b}_n)$ são linearmente independentes.

(ii) Suponha que f seja sobrejetor e que $\mathbf{b}_1, \dots, \mathbf{b}_n$ gerem V. Prove que $f(\mathbf{b}_1), \dots, f(\mathbf{b}_n)$ geram W.

(iii) Suponha agora que f seja bijetor. Prove que $\dim V = \dim W$.

E74 Sejam V e W espaços vetoriais e $f\colon V \to W$ uma função linear. Seja $W^* = \operatorname{Im} f$. Seja $V^* \subset V$ um complemento de $\operatorname{Ker} f$ em V, isto é, suponha que $V = \operatorname{Ker} f \oplus V^*$. Defina $f^*\colon V^* \to W^*$ pondo $f^*(\mathbf{v}) = f(\mathbf{v})$ para todo $\mathbf{v} \in V^*$. Prove que f^* é bijetora. Deduza que

$$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim V. \tag{56}$$

[*Observação.* Este exercício dá uma prova alternativa para o teorema núcleo-imagem.]

E75 Denotemos o posto de uma matriz M por $\operatorname{posto} M$.

(i) Sejam $A \in \mathbb{F}^{R\times S}$ e $B \in \mathbb{F}^{S\times T}$ matrizes. Prove que

$$\operatorname{posto}(AB) \le \min\{\operatorname{posto} A, \operatorname{posto} B\}. \tag{57}$$

(ii) Dê exemplos de matrizes A e B para os quais (57) vale com desigualdade estrita.

(iii) Suponha que $A \in \mathbb{F}^{m\times n}$ e $B \in \mathbb{F}^{n\times m}$ são tais $AB = I_m$ e $BA = I_n$, onde I_m e I_n são as matrizes identidade. Prove que $m = n$.

(iv) Suponha que $M \in \mathbb{F}^{m\times n}$ seja inversível. Prove que $m = n$.

{*Data de entrega*: 3/11/2024}

E76 Seja $I_n \in \mathbb{F}^{n\times n}$ a matriz identidade.

(i) Seja $A \in \mathbb{F}^{n\times n}$ uma matriz com $\operatorname{posto} A = n$. Prove que existe uma única matriz $Q \in \mathbb{F}^{n\times n}$ tal que $AQ = I_n$.

(ii) Seja $B \in \mathbb{F}^{n\times n}$ uma matriz com $\operatorname{posto} B = n$. Prove que existe uma única matriz $P \in \mathbb{F}^{n\times n}$ tal que $PB = I_n$.

(iii) Seja $M \in \mathbb{F}^{n\times n}$ uma matriz com $\operatorname{posto} M = n$. Prove que existe uma única matriz $N \in \mathbb{F}^{n\times n}$ tal que $NM = MN = I_n$.

E77 (M) Lembre que $\mathbb{R}$ é um espaço vetorial sobre $\mathbb{Q}$ (veja o Exercício **E15**). Seja $f\colon \mathbb{R} \to \mathbb{R}$ uma função linear, com $\mathbb{R}$ sendo considerado como um espaço vetorial sobre $\mathbb{Q}$ (isto é, f preserva somas e f é $\mathbb{Q}$-linear: $f(\alpha r) = \alpha f(r)$ para todo $\alpha \in \mathbb{Q}$ e $r \in \mathbb{R}$). É verdade que f é contínua? É verdade que f é contínua em $0 \in \mathbb{R}$?

E78 Sejam U e W subespaços de $V \subset \mathbb{F}^D$, com D finito. Suponha que U e W são complementares em V, de forma que $V = U \oplus W$. Suponha que, para um subespaço $W' \subset V$, também vale que U e W' são complementares em V.

(i) É verdade que, necessariamente, $W = W'$? Prove ou dê contraexemplo.

(ii) É verdade que, necessariamente, $\dim W = \dim W'$? Prove ou dê contraexemplo.

E79 Sejam U e V espaços vetoriais e seja $f\colon U \to V$ uma função linear. Seja $\sim$ a relação definida sobre U tal que, para quaisquer $\mathbf{u}$ e $\mathbf{u}'$ em U, temos $\mathbf{u} \sim \mathbf{u}'$ se e só se $\mathbf{u} - \mathbf{u}' \in \operatorname{Ker} f$. Prove que $\sim$ é uma relação de equivalência.

E80 (Continuação de **E79**) Para $\mathbf{u} \in U$, seja $[\mathbf{u}]$ a classe de equivalência de $\mathbf{u}$ relativa à relação $\sim$:
$$[\mathbf{u}] = \{\mathbf{u}' \in U : \mathbf{u}' \sim \mathbf{u}\}. \tag{58}$$

(*i*) Prove que, para todo $\mathbf{u} \in U$, temos
$$[\mathbf{u}] = \mathbf{u} + \operatorname{Ker} f. \tag{59}$$

(*ii*) Seja
$$U/{\sim} = \big\{[\mathbf{u}] : \mathbf{u} \in U\big\}. \tag{60}$$
Lembre que existe U^* subespaço de U tal que $U = U^* \oplus \operatorname{Ker} f$. Considere a função $\pi : U^* \to U/{\sim}$ tal que $\pi(\mathbf{u}) = [\mathbf{u}]$ para todo $\mathbf{u} \in U^*$. Prove que π é uma bijeção.

E81 (Continuação de **E80**) Existe uma forma natural de se definir soma e produto por escalar em $U/{\sim}$ que tornam $U/{\sim}$ um espaço vetorial: $[\mathbf{u}] + [\mathbf{u}'] = [\mathbf{u} + \mathbf{u}']$ e $\alpha[\mathbf{u}] = [\alpha\mathbf{u}]$ para quaisquer $\mathbf{u}$ e $\mathbf{u}'$ em U e α escalar (é necessário verificar (exercício) que essas operações estão bem definidas, pois elas estão sendo definidas em termos de representantes de classe, e precisamos provar que estas definições não dependem dos representantes escolhidos). Prove que a função π do Exercício **E80** é linear. Conclua que a função
$$f^* \circ \pi^{-1} : U/{\sim} \to \operatorname{Im} f \tag{61}$$
é linear e bijetora. Aqui, $f^* : U^* \to \operatorname{Im} f$ é a função tal que $f^*(\mathbf{u}) = f(\mathbf{u})$ para todo $\mathbf{u} \in U^*$. [*Observação.* Este exercício diz que o espaço quociente $U/{\sim}$ é isomorfo ao espaço $\operatorname{Im} f$.]

E82 Lembre-se do Exercício **E61**. Seja X um conjunto finito, e suponha que $\mathcal{F} \subset \mathcal{P}(X)$ é tal que $|F \cap F'|$ é par para quaisquer dois F e F' membros de $\mathcal{F}$. Prove que $|\mathcal{F}| \leq 2^{\lfloor |X|/2 \rfloor}$. [*Sugestão.* Considere $U = \big\{\mathbb{1}_F \in \mathrm{GF}(2)^X : F \in \mathcal{F}\big\}$ e seu aniquilador U°.] **{*Data de entrega*: 10/11/2024}**

E83 Dadas uma matrix $A \in \mathbb{R}^{m\times n}$ e um vetor $\mathbf{b} \in \mathbb{R}^m$, seja $\mathrm{Sol}(A, \mathbf{b}) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{b}\}$. Para cada uma das afirmações abaixo, prove a afirmação ou prove que não existem os objetos descritos.

(*i*) Exitem uma matriz escalonada $U \in \mathbb{R}^{3\times 4}$ e $\mathbf{b} \in \mathbb{R}^3$ tais que $\mathrm{Sol}(U, \mathbf{b})$ é vazio.

(*ii*) Existem uma matriz escalonada $U \in \mathbb{R}^{3\times 4}$ e $\mathbf{b} \in \mathbb{R}^3$ tais que $\mathrm{Sol}(U, \mathbf{b})$ tem exatamente um elemento.

(*iii*) Existem uma matriz escalonada $U \in \mathbb{R}^{3\times 4}$ e $\mathbf{b} \in \mathbb{R}^3$ tais que $\mathrm{Sol}(U, \mathbf{b})$ tem infinitos elementos.

{*Data de entrega*: 10/11/2024}

E84 No que segue, escrevemos $[m]$ para o conjunto $\{1, 2, \ldots, m\}$ para qualquer inteiro m. Seja $\sigma : [m] \to [m]$ uma permutação (isto é, uma bijeção). Seja $P_\sigma = (a_{ij})$ a matriz $m \times m$ tal que, para todo $i \in [m]$,
$$a_{ij} = \begin{cases} 1 & \text{se } j = \sigma(i) \\ 0 & \text{caso contrário.} \end{cases} \tag{62}$$
Seja $A \in \mathbb{F}^{m\times n}$ uma matriz.

(*i*) Descreva a matriz $P_\sigma A$ em termos das linhas de A. Isto é, pense em A da seguinte forma:

$$A = \begin{bmatrix} A_{1*} \\ A_{2*} \\ \vdots \\ A_{m*} \end{bmatrix}, \tag{63}$$

onde A_{i*} é a i-ésima linha de A, e descreva $P_\sigma A$ em termos dos A_{i*}.

(*ii*) Suponha agora que temos uma permutação $\tau\colon [n] \to [n]$. Pensemos agora em A em termos de suas colunas:

$$A = \begin{bmatrix} A_{*1} & A_{*2} & \dots & A_{*n} \end{bmatrix}, \tag{64}$$

onde A_{*j} é a j-ésima coluna de A. Defina uma matriz Q_τ parecida com a matriz P_σ acima de forma que

$$AQ_\tau = \begin{bmatrix} A_{*\tau(1)} & A_{*\tau(2)} & \dots & A_{*\tau(n)} \end{bmatrix}. \tag{65}$$

E85 Considere a matriz

$$A = \begin{bmatrix} 0 & 2 & 4 & 2 & 8 \\ 2 & 1 & 0 & 5 & 4 \\ 4 & 1 & 2 & 4 & 2 \\ 5 & 0 & 0 & 2 & 8 \end{bmatrix}, \tag{66}$$

que ocorre no Exemplo 7.3.3 de **PNK**.

(*i*) Continue o processo de escalonamento de A naquele exemplo, para obter a matriz escalonada

$$U = \begin{bmatrix} 2 & 1 & 0 & 5 & 4 \\ 0 & 2 & 4 & 2 & 8 \\ 0 & 0 & 4 & -5 & -2 \\ 0 & 0 & 0 & -1.75 & 10.5 \end{bmatrix}. \tag{67}$$

Descreva claramente os passos (adicionais) que você executou para completar esse escalonamento.

(*ii*) Encontre um matriz inversível M tal que $MA = U$.

(*iii*) Monte agora a matriz

$$A' = \begin{bmatrix} A & I \end{bmatrix}, \tag{68}$$

com 4 linhas e 9 colunas, onde I é a matriz identidade 4×4. Execute novamente os passos do processo de escalonamento que levam A a U, mas agora na matriz A' (por exemplo, o primeiro passo é multiplicar a segunda linha por -2 e somar o resultado à terceira linha; você deve executar exatamente o mesmo processo com a matriz 'estendida' A' no primeiro passo do processo). Ao terminar este processo, você terá uma matriz da forma

$$U' = \begin{bmatrix} U & B \end{bmatrix}, \tag{69}$$

onde B é uma certa matriz 4×4. É natural que a 'primeira parte' de U' seja U, pois executamos exatamente o mesmo processo de escalonamento. Entretanto, o que você obteve como B?

(*iv*) Explique por que o fato que você observou no item anterior não é coincidência, e de fato sempre ocorre. [*Observação.* Note que isto dá um bom algoritmo para se obter M "com lápis e papel".]

E86 Seja $V \subset \mathbb{F}^D$ um espaço vetorial, onde D é finito. Seja $I \subset V$ um conjunto de vetores linearmente independentes. Prove que é possível estender I a uma base B de V (isto é, prove que existe B base de V com $I \subset B$). [*Sugestão.* Você pode considerar uma variante apropriada de Grow e provar que tal algoritmo necessariamente termina com uma base B como queremos. Você pode também considerar conjuntos linearmente independentes $B \subset V$ com $I \subset B$ com $|B|$ o maior possível e argumentar que tais conjuntos são como queremos. De qualquer forma, diga explicitamente onde você usou a hipótese que D é finito.]

E87 Sejam U e V subespaços de $\mathbb{F}^D$, com D finito. Defina o conjunto $U + V \subset \mathbb{F}^D$ pondo

$$U + V = \{u + v \colon u \in U \text{ e } v \in V\}. \tag{70}$$

Isto é, os elementos de $U + V$ são todas as somas $u + v$ com $u \in U$ e $v \in V$.

(*i*) Prove que $U + V$ é um espaço vetorial.

(*ii*) Prove que

$$\dim(U + V) + \dim(U \cap V) = \dim U + \dim V. \tag{71}$$

[*Sugestão.* Verifique $U \cap V$ é um espaço vetorial. Considere uma base B de $U \cap V$. Estenda B a uma base B_U de U. Estenda B a uma base B_V de V. Prove que $B_U \cup B_V$ é uma base de $U + V$.]

{*Data de entrega*: 24/11/2024}

E88 Para $\mathbf{v} \in \mathbb{F}^{\mathbb{N}}$, seja $\operatorname{supp} \mathbf{v} = \{i \in \mathbb{N} \colon \mathbf{v}(i) \neq 0\}$. Seja

$$V = \{\mathbf{v} \in \mathbb{F}^N \colon \operatorname{supp} \mathbf{v} \text{ é um conjunto finito}\}. \tag{72}$$

Note que o produto $\mathbf{u} \cdot \mathbf{v} = \sum_{i \in \mathbb{N}} \mathbf{u}(i)\mathbf{v}(i)$ está bem definido em V, de forma que, dado um subespaço U de V, podemos definir

$$U^\circ = \{\mathbf{v} \in V \colon \mathbf{v} \cdot \mathbf{u} = 0 \text{ para todo } \mathbf{u} \in U\} \tag{73}$$

de forma usual.

Para cada $i < j$ naturais, seja $\mathbf{v}_{ij} \colon \mathbb{N} \to \mathbb{F}$ com $\mathbf{v}_{ij}(i) = -1$ e $\mathbf{v}_{ij}(j) = 1$. Seja $U = \operatorname{Span}\{\mathbf{v}_{ij} \colon i < j\}$ o espaço vetorial gerado por tais vetores $\mathbf{v}_{ij}$. Note que $U \subset V$.

(*i*) Determine U°.

(*ii*) Determine $(U^\circ)^\circ$.

(*iii*) É verdade que $(U^\circ)^\circ = U$?

E89 Vimos que é de interesse termos um algoritmo, que chamamos de Algoritmo X, que, ao receber vetores $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{F}^n$, devolve um conjunto gerador para o aniquilador V° de $V = \operatorname{Span}\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$.

(*i*) Descreva como podemos implementar o Algoritmo X usando como subrotina o processo de eliminação de Gauss. Seu algoritmo encontra uma base de V°?

(*ii*) Prove que seu Algoritmo X está correto.

(*iii*) Codifique seu Algoritmo X em Python.

E90 (i) Considere a matriz

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \in \mathrm{GF}(2)^{3\times 5}. \tag{74}$$

Encontre uma base para $\mathrm{Null}\, A$.

(ii) Considere a matriz

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \in \mathrm{GF}(2)^{2\times 5}. \tag{75}$$

Encontre uma matriz A com entradas em $\mathrm{GF}(2)$ tal que $\mathrm{Null}\, A = \mathrm{Row}\, B$.

[*Observação.* Em ambos os itens acima, justifique sua resposta.] **{*Data de entrega*: 24/11/2024}**

E91 Sejam $M \in \mathbb{F}^{a\times b}$ e $A \in \mathbb{F}^{b\times c}$ duas matrizes.

(i) Prove que $\mathrm{posto}(MA) \le \mathrm{posto}\, A$.

(ii) Prove que, se M é inversível, então $\mathrm{posto}(MA) = \mathrm{posto}\, A$.

E92 Sejam $A \in \mathbb{F}^{R\times S}$ e $B \in \mathbb{F}^{S\times T}$ duas matrizes. Sejam A_{*s} $(s \in S)$ as colunas de A e B_{s*} $(s \in S)$ as linhas de B (essa notação é como em (63) e (64)). Prove que

$$AB = \sum_{s\in S} A_{*s}B_{s*}. \tag{76}$$

Note que AB e $A_{*s}B_{s*}$ $(s \in S)$ são matrizes $R \times T$.

E93 Sejam $\mathbf{q}_1, \dots, \mathbf{q}_k \in \mathbb{R}^n$ vetores unitários mutualmente ortogonais. Seja $M = \sum_{1\le i\le k} \mathbf{q}\mathbf{q}^\top$. Note que M é uma matriz $n \times n$. Seja $V = \mathrm{Span}\{\mathbf{q}_1, \dots, \mathbf{q}_k\}$ e, para todo $\mathbf{b} \in \mathbb{R}^n$, considere a decomposição $\mathbf{b} = \mathbf{b}^{\parallel V} + \mathbf{b}^{\perp V}$ com $\mathbf{b}^{\parallel V} \in V$ e $\mathbf{b}^{\perp V}$ ortogonal a V. Prove que $M\mathbf{b} = \mathbf{b}^{\parallel V}$. [*Sugestão.* Você pode usar que $\mathbf{q}^\top\mathbf{b} = \langle \mathbf{b}, \mathbf{q}\rangle$ e então verificar que $M\mathbf{b}$ e $\mathbf{b} - M\mathbf{b}$ satisfazem as propriedades que definem a decomposição de $\mathbf{b}$. Alternativamente, você pode usar **E92** e invocar uma fórmula matricial que provamos para $\mathbf{b}^{\parallel V}$.]

E94 Seja W um subespaço vetorial de $\mathbb{R}^n$. Seja U um subespaço vetorial de W, e seja $U^\perp$ o complemento ortogonal de U, isto é,

$$U^\perp = \{\mathbf{w} \in W : \langle \mathbf{w}, \mathbf{u}\rangle = 0 \text{ para todo } \mathbf{u} \in U\}. \tag{77}$$

(i) Prove que $U \subset (U^\perp)^\perp$.

(ii) Prove que $W = U \oplus U^\perp$ e deduza que $\dim U + \dim U^\perp = \dim W$.

(iii) Prove que $U = (U^\perp)^\perp$ usando um argumento de dimensão apropriado.

[*Observação.* Como estamos usando o produto interno padrão $\langle \mathbf{x}, \mathbf{y}\rangle = \mathbf{x}\cdot\mathbf{y}$, este exercício basicamente segue de nosso estudo de aniquiladores (ele segue imediatamente no caso em que $W = \mathbb{R}^n$). Entretanto, é interessante fazer este exercício supondo que temos um produto interno abstrato (e não necessariamente o *dot product*).]

E95 Seja $U \subset \mathrm{GF}(2)^n$ um espaço vetorial.

(i) Vale necessariamente que $\mathrm{GF}(2)^n = U \oplus U^\circ$?

(ii) Vale necessariamente que $\dim U + \dim U^\circ = n$?

E96 Seja M uma matriz $n \times n$ triangular superior, com todos seus elementos diagonais iguais a 1. Prove que M é inversível e que sua inversa M^{-1} é triangular superior, com todos seus elementos diagonais iguais a 1.

E97 (i) Sejam $\mathbf{v}_1$ e $\mathbf{v}_2 \in \mathbb{R}^3$ dois vetores ortonormais, isto é, tais que $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = 0$ e $\|\mathbf{v}_i\| = 1$ para $i \in \{1, 2\}$. Seja $M = [\mathbf{v}_1\ \mathbf{v}_2] \in \mathbb{R}^{3\times 2}$ a matriz cujas colunas são os vetores $\mathbf{v}_i$. Verifique que $M^\top M$ é uma matriz identidade. Prove que $MM^\top$ não é uma matriz identidade.

(ii) Sejam $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{R}^n$ vetores ortonormais, isto é, tais que $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ para todo $i \neq j$ e $\|\mathbf{v}_i\| = 1$ para todo i. Seja $M = [\mathbf{v}_1\ \dots\ \mathbf{v}_n] \in \mathbb{R}^{n\times n}$ a matriz quadrada cujas colunas são os vetores $\mathbf{v}_i$. Verifique que $M^\top M = I_n$, onde I_n é a matriz identidade $n \times n$. Prove que M é uma matriz inversível, que $M^{-1} = M^\top$ e que $MM^\top = I_n$.

***{Data de entrega*: 1/12/2024}**

E98 Seja $A \in \mathbb{R}^{m\times n}$ uma matriz cujas colunas são linearmente independentes. Prove que $A^\top A$ é uma matriz inversível. [*Sugestão.* Lembre que A pode ser escrita como um produto QR onde Q tem colunas ortonormais e R é uma matriz inversível. Use esse fato.]

E99 Seja $A \in \mathbb{F}^{m\times n}$ uma matriz cujas colunas são linearmente independentes. É necessariamente verdade que $A^\top A$ é uma matriz inversível? Prove ou dê um contraexemplo. [*Observação.* Note que aqui você não pode usar a fatoração QR, pois estamos em um corpo arbitrário $\mathbb{F}$.] ***{Data de entrega*: 8/12/2024}**

E100 Neste exercício, como de usual, consideramos o produto interno padrão do $\mathbb{R}^n$, de forma que $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{y}^\top \mathbf{x} = \mathbf{x} \cdot \mathbf{y}$ para $\mathbf{x}$, $\mathbf{y} \in \mathbb{R}^n$. Dizemos que uma matriz $A \in \mathbb{R}^{n\times n}$ *preserva* o produto interno se, para todo $\mathbf{x}$ e $\mathbf{y}$ em $\mathbb{R}^n$, vale que $\langle A\mathbf{x}, A\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$. Prove as seguintes asserções:

(i) Se A é ortogonal, então A preserva o produto interno.

(ii) Se A preserva o produto interno, então A preserva a norma, isto é, para todo $\mathbf{x} \in \mathbb{R}^n$, vale que $\|A\mathbf{x}\| = \|\mathbf{x}\|$.

(iii) Se A preserva a norma, então A é ortogonal. [*Sugestão.* Calcule $\langle A(\mathbf{x}+\mathbf{y}), A(\mathbf{x}+\mathbf{y}) \rangle$.]

E101 Seja $\mathbb{F}$ um corpo infinito arbitrário. Suponha que $U_1, \dots, U_k$ sejam subespaços de $\mathbb{F}^n$ com $\dim U_i < n$ para todo i. Prove que $\bigcup_{1\le i\le k} U_i \neq \mathbb{F}^n$. [*Observação.* A primeira solução satisfatória desse exercício vale um prêmio chocolático. Você pode usar o fato que um polinômio $p(X)$ de grau d com coeficientes em $\mathbb{F}$ tem no máximo d raízes.]

E102 Sejam $\mathbf{a}_1, \dots, \mathbf{a}_t$ vetores em $\mathbb{R}^n$. Dizemos esses vetores são *quase-co-hiperplanares*, se existem $\mathbf{a}'_1, \dots, \mathbf{a}'_t \in \mathbb{R}^n$ e $\mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ tais que, para todo i,

$$\|\mathbf{a}'_i - \mathbf{a}_i\| \le 10^{-10}\|\mathbf{a}_i\| \tag{78}$$

e

$$\langle \mathbf{a}'_i, \mathbf{x} \rangle = 0. \tag{79}$$

Naturalmente, (79) significa que os $\mathbf{a}'_i$ pertencem ao hiperplano ortogonal a $\mathbf{x}$. Grosso modo, os $\mathbf{a}_i$ ($1 \le i \le t$) são quase-co-hiperplanares se uma 'pequena perturbação' $\mathbf{a}'_i$ deles são co-hiperplanares (pertencem a um mesmo subespaço de dimensão $n-1$ de $\mathbb{R}^n$). Prove que os vetores da base canônica $\mathbf{e}_1, \dots, \mathbf{e}_n \in \mathbb{R}^n$ são quase-co-hiperplanares se $n \ge 10^{20}$.

E103 Sejam $\varphi = (1 + \sqrt{5})/2$ e $\psi = (1 - \sqrt{5})/2$. Seja

$$S = \begin{bmatrix} \varphi & \psi \\ 1 & 1 \end{bmatrix}. \tag{80}$$

(*i*) Seja

$$T = \begin{bmatrix} 1/\sqrt{5} & (1-1/\sqrt{5})/2 \\ -1/\sqrt{5} & (1+1/\sqrt{5})/2 \end{bmatrix}. \tag{81}$$

Verifique que $T = S^{-1}$.

(*ii*) Sejam

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{e} \quad \mathbf{u}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{82}$$

Defina $\mathbf{u}_t = A^{t-1}\mathbf{u}_1$ para todo $t \geq 1$. Prove que $\mathbf{u}_t = [F_t\ F_{t-1}]^\top$ para todo $t \geq 1$, onde F_n é o n-ésimo número de Fibonacci ($F_n = n$ para $n \in \{0,1\}$ e $F_n = F_{n-1}+F_{n-2}$ para todo $n \geq 2$).

(*iii*) Calcule $S^{-1}AS$.

(*iv*) Use os itens anteriores para provar que

$$F_t = \frac{1}{\sqrt{5}}(\varphi^t - \psi^t) \tag{83}$$

para todo $t \geq 0$.

E104 Seja $A = (a_{ij}) \in \mathbb{F}^{n\times n}$ uma matriz triangular superior, isto é, tal que $a_{ij} = 0$ se $i > j$. Ademais, suponha que alguma entrada diagonal de A seja nula ($a_{ii} = 0$ para pelo menos um índice i). Prove que A não é inversível.

E105 Seja $A = (a_{ij}) \in \mathbb{F}^{n\times n}$ uma matriz triangular superior. Suponha que alguma entrada diagonal de A seja λ. Prove que λ é um autovalor de A.

E106 Seja $A \in \mathbb{F}^{n\times n}$ uma matriz diagonalizável. Considere a função linear $f_A\colon \mathbb{F}^n \to \mathbb{F}^n$ associada a A usual, dada for $f_A(\mathbf{v}) = A\mathbf{v}$ para todo $\mathbf{v} \in \mathbb{F}^n$. Prove que existe uma base $\mathbf{v}_1, \dots, \mathbf{v}_n$ de $\mathbb{F}^n$ e escalares $\lambda_1, \dots, \lambda_n$ tais que $f_A(\mathbf{v}_i) = \lambda_i\mathbf{v}_i$ para todo i. De forma mais geral, dê uma fórmula para $f_A(\mathbf{v})$, escrevendo $\mathbf{v}$ em termos dos $\mathbf{v}_i$ ($1 \leq i \leq n$). **{*Data de entrega*: 8/12/2024}**

E107 Seja $A \in \mathbb{F}^{n\times n}$ uma matriz e λ um autovalor de A. O *autoespaço* de A associado a λ é

$$V_\lambda = \{\mathbf{v} \in \mathbb{F}^n \colon A\mathbf{v} = \lambda\mathbf{v}\}. \tag{84}$$

(*i*) Prove que V_λ é um espaço vetorial

(*ii*) Sejam λ e λ' autovalores de A distintos. Prove que os autoespaços correspondentes V_λ e $V_{\lambda'}$ tem interseção trivial: $V_\lambda \cap V_{\lambda'} = \{\mathbf{0}\}$.

E108 Seja $A \in \mathbb{F}^{n\times n}$ uma matriz.

(*i*) Suponha que $\lambda_1, \dots, \lambda_m$ sejam autovalores distintos de A. Sejam $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbb{F}^n \setminus \{\mathbf{0}\}$ tais que, para cada $1 \leq i \leq m$, o vetor $\mathbf{v}_i$ pertence ao autoespaço V_{λ_i} de A (veja (84)). Prove que os vetores $\mathbf{v}_1, \dots, \mathbf{v}_m$ são linearmente independentes. [*Sugestão.* Prove por indução em k que $\mathbf{v}_1, \dots, \mathbf{v}_k$ são linearmente independentes.]

(*ii*) Prove que a matriz A tem no máximo n autovalores distintos.

{*Data de entrega*: 8/12/2024}

E109 Suponha que $A \in \mathbb{F}^{n\times n}$ tenha n autovalores distintos. Prove que A é diagonalizável.

E110 (*i*) Sejam $A \in \mathbb{F}^{r\times s}$ e $B \in \mathbb{F}^{s\times t}$. Prove que $(AB)^\top = B^\top A^\top$.

(*ii*) Suponha que $A \in \mathbb{F}^{n\times n}$ seja uma matriz inversível. Prove que $A^\top$ é inversível e que $(A^\top)^{-1} = (A^{-1})^\top$.

(*iii*) Suponha que $A \in \mathbb{F}^{n\times n}$ seja uma matriz diagonalizável. Prove que $A^\top$ é diagonalizável.