

PROVA DISCURSIVA

- Nesta prova, faça o que se pede, usando, caso deseje, os espaços para rascunho indicados no presente caderno. Em seguida, transcreva os textos para o **CADERNO DE TEXTOS DEFINITIVOS DA PROVA DISCURSIVA**, nos locais apropriados, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto que ultrapassar a extensão máxima de linhas disponibilizadas será desconsiderado. Também será desconsiderado o texto que não for escrito na(s) **folha(s) de texto definitivo** correspondente(s).
- No **Caderno de Textos Definitivos**, identifique-se apenas no cabeçalho da primeira página, pois não será avaliado texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado. Caso queira assinar seus textos, utilize apenas o nome **Oficial Técnico de Inteligência**. Ao texto que contenha outra forma de identificação será atribuída nota zero, correspondente à identificação do candidato em local indevido.
- Na avaliação da dissertação, ao domínio do conteúdo serão atribuídos até **90,00 pontos**, dos quais até **4,50 pontos** serão destinados ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado). Na avaliação de cada questão, esses valores corresponderão a **30,00 pontos** e **1,50 ponto**, respectivamente.

DISSERTAÇÃO

Uma importante aplicação da Álgebra Linear à Estatística está na dedução da fórmula de estimação dos coeficientes de um modelo de regressão linear que relacione uma variável dependente Y a n variáveis independentes X_1, X_2, \dots, X_n , como se segue:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \dots + \beta_n X_n + \varepsilon,$$

em que ε é chamada perturbação, que reflete a diferença entre os valores calculados pela relação linear em função das variáveis independentes e o valor real de Y .

Para produzir uma estimativa dos coeficientes do modelo linear, seja $\boldsymbol{\beta} = (\beta_0, \beta_1, \beta_2, \dots, \beta_n)^T$ o vetor dos coeficientes da equação real e seja $\mathbf{b} = (b_0, b_1, b_2, \dots, b_n)^T$ a estimativa calculada pelo método dos mínimos quadrados (o sobrescrito T indica a transposição de vetor). Se forem tomadas m amostras dos valores correspondentes de $X_1, X_2, X_3, \dots, X_n, Y$, com $m > n + 1$, então podem ser montados: (i) uma matriz \mathbf{X} com m linhas e $n + 1$ colunas formada por uma coluna com m entradas iguais a 1 (que pode ser interpretada como uma variável X_0 que assume sempre o mesmo valor 1 e é multiplicada pelo coeficiente β_0 no modelo linear) e por mais n colunas determinadas pelos valores de todos os X_j , sendo cada linha correspondente a uma observação, e (ii) um vetor-coluna \mathbf{y} formado pelos m valores observados de Y , ordenados conforme a ordem das linhas da matriz \mathbf{X} .

A estimativa de mínimos quadrados de $\boldsymbol{\beta}$ é aquela que faz que os resíduos resultantes (estimativas das perturbações) tenham a menor soma dos quadrados possível. Usando métodos de Cálculo e de Álgebra Linear, essa estimativa é dada pela fórmula: $\mathbf{b} = (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \mathbf{y}$.

Com esse vetor de coeficientes estimados, podem-se calcular um vetor $\hat{\mathbf{y}}$ de estimativas de Y e um vetor \mathbf{e} de resíduos estimados, dados por: $\mathbf{e} = \mathbf{y} - \hat{\mathbf{y}}$ em que $\hat{\mathbf{y}} = \mathbf{X}\mathbf{b}$.

Dois importantes pressupostos para esta aplicação da Álgebra Linear são que \mathbf{X} tenha posto máximo $n + 1$ e que a soma dos resíduos estimados, elementos do vetor \mathbf{e} , seja nula, isto é, $e_1 + e_2 + \dots + e_m = 0$.

Com base no texto acima e com as convenções e notações ali apresentadas, e especificando outras que julgue necessárias, redija um texto dissertativo a respeito dos aspectos algébricos do método dos mínimos quadrados, descrevendo-os minuciosamente.

Em seu texto, aborde os seguintes aspectos:

- 1 a adequação dimensional dos produtos matriciais apresentados; [valor: 20,00 pontos]
- 2 o significado e a necessidade de a matriz \mathbf{X} ter posto máximo; [valor: 35,50 pontos]
- 3 a forma como o pressuposto de soma nula dos resíduos é atendido pela fórmula de estimação de \mathbf{b} . [valor: 30,00 pontos]

DISSERTAÇÃO – RASCUNHO – 1/2

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

DISSERTAÇÃO – RASCUNHO – 2/2

31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	

QUESTÃO 1

O conceito de entropia pode ser considerado como uma das grandes realizações das ciências. A entropia constitui a essência da mecânica estatística e também exerce papel central na teoria da informação. A sua interpretação física beneficia outras áreas do conhecimento, como filosofia, economia e computação. A importante inovação de Shannon, proposta em 1948, tem o objetivo de mostrar que o conceito de entropia não se restringe apenas à termodinâmica, mas pode ser aplicado no contexto que envolva probabilidades. Assim, o conceito de entropia permeia diferentes áreas do conhecimento, tais como biologia, economia, sociologia, psicologia e, até mesmo, as artes.

Paulo Sérgio Almeida-Santos *et al.* **Utilização da entropia informacional na seleção de indicadores financeiros mais relevantes para tomada de decisão no setor público: o caso dos estados brasileiros.** *In: Perspectivas em Ciência da Informação.* Belo Horizonte, v. 19, n.º 2, abr./jun./2014, p. 83-105 (com adaptações).

Hoje, há diversas outras definições de entropia, como a diferencial e a de Tsallis, bastante úteis para o estudo de processos aleatórios. Por exemplo, a distribuição exponencial, que surge naturalmente quando se modela o intervalo de tempo entre duas ocorrências consecutivas em um processo de Poisson homogêneo, também pode ser deduzida com base no conceito de entropia diferencial.

Considerando que o texto apresentado tem caráter unicamente motivador, redija um texto acerca de tecnologia da informação, atendendo ao que se pede a seguir.

- 1 Defina entropia de Shannon (S) e entropia diferencial (D) e explique o significado dos casos $S = 0$ e $D = 0$; [valor: 12,00 pontos]
 - 2 Determine a entropia diferencial de uma distribuição exponencial; [valor: 9,50 pontos]
 - 3 Demonstre que a distribuição exponencial é uma distribuição de máxima entropia. [valor: 7,00 pontos]
-

QUESTÃO 1 – RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

QUESTÃO 2

Uma empresa irá efetuar a compra de muitos dispositivos móveis para seus empregados e precisa que sua área de segurança da informação avalie os riscos no uso desse tipo de dispositivo, em relação a confidencialidade e a integridade dos dados que serão armazenados e enviados a partir deles, e utilize recursos de criptografia para ajudar a diminuir os riscos. Os empregados deverão utilizar *emails*, editores de textos e planilhas nesses dispositivos.

Com base nas informações apresentadas na situação hipotética descrita, redija um texto dissertativo acerca do funcionamento dos recursos criptográficos e dos algoritmos para ajudar a diminuir os riscos de confidencialidade e da integridade dos dados que serão armazenados, enviados e recebidos pelos dispositivos citados. Em seu texto, aborde os seguintes tópicos:

- 1 envio de *emails* com o uso de assinatura digital; [valor: 8,00 pontos]
- 2 conceito de função de *hash* criptográfica; [valor: 8,00 pontos]
- 3 uso do algoritmo SHA-512 e etapas de processamento desse algoritmo. [valor: 12,50 pontos]

QUESTÃO 2 – RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	