

DEPARTAMENTO DE TECNOLOGÍA INFORMÁTICA Y COMPUTACIÓN

Examen

MATEMÁTICA DISCRETA

14-09-2007

1.- (a) Define el código Gray, da su interpretación en términos de teoría de grafos y completa uno de longitud 3. (0.45 puntos)

(b) Enuncia los resultados que caracterizan la existencia de un tour Euleriano y de un camino Euleriano en un grafo no dirigido. Haz lo mismo para el caso de un grafo dirigido. (0.8 puntos)

(c) Dada la expresión algebraica $\left(\sqrt{x^2 - v^3}\right) \left(4a - \left(\frac{1}{b} + e_4\right)\right)$. Obtén el árbol que representa esta expresión. Utiliza el algoritmo de preorden (explicando cada uno de los pasos) para calcular la notación polaca directa o notación prefija correspondiente a esta expresión algebraica. (0.75 puntos).

2.- Una compañía de reforestación sembrará arboles en zonas vacías de la misma Área.

Por eso ha desarrollado un sistema de caminos de tierra para Tener acceso a cualquier zona desde cualquier otra. La Distancia entre cada pareja de zonas viene dada en la tabla Adjunta. Utiliza el algoritmo de Prim para adivinar entre Que pares de zonas deben de construirse caminos para Conectarlas todas con una longitud total mínima de caminos. Indica además cual es longitud total mínima de camino que Se tiene que construir.

. (2 puntos)

	1	2	3	4	5	6	7	8
1	-	13	21	9	7	18	20	15
2		-	9	18	12	26	23	11
3			-	26	17	25	19	10
4				-	7	16	15	9
5					-	9	11	8
6						-	6	10
7							-	5
8								-

3.- Consideramos un representado por la matriz de adyacencia adjunta.

$$A = \begin{bmatrix} 0.1 & 0.1 & 1.1 \\ 0.0 & 0.2 & 2.0 \\ 1.1 & 0.1 & 1.1 \\ 0.1 & 0.0 & 0.0 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

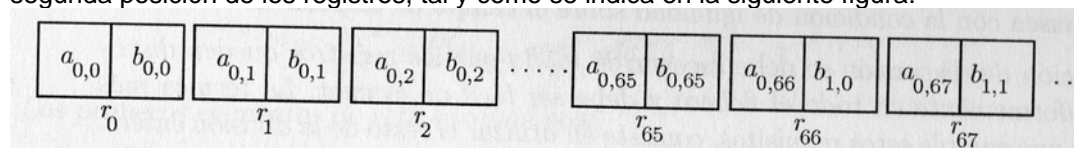
(a) Aplica el algoritmo de Warshall a este grafo. (0.75 puntos).

(b) ¿Cómo se llama la matriz que resulta de este algoritmo y que representa? Indica concretamente el significado de la fila 5 de la matriz que se obtiene al realizar el algoritmo de Warshall. (0.5 puntos).

(c) Calcula las componentes conexas asociadas al grafo. Dibuja los grafos que correspondan a estas componentes conexas (0.75)

4.- Disponemos de dos raíces $A = (a_{ij})_{i,j=0}^{167}$ y $B = (b_{ij})_{i,j=0}^{65}$ de dos dimensiones. La raíz A es de dimensión 168x168 y la raíz B tiene la dimensión 66x66. Suponemos numeradas las filas y columnas de ambas raíces a partir de Q.

Disponemos además de unos tipos de registros dobles $r_i, i \geq 0$ capaces de almacenar dos datos en las posiciones 1 y 2. Supongamos que los elementos de la raíz A se almacenan consecutivamente por filas en la primera posición de los registros, mientras que los elementos de la raíz B se almacenan también consecutivamente por filas en la segunda posición de los registros, tal y como se indica en la siguiente figura:



Determina qué registros contienen simultáneamente elementos de la columna numero 60 la raíz A y elementos de la columna número 18 de la raíz B. (Recuerda que las posiciones se cuentan a partir de 0). Es necesario enfocar el problema a partir de conceptos vistos en clase (2 puntos) (NOTA: pag.243-244).

5.- (a) Explica las diferencias entre los sistemas criptográficos de clave privada y clave pública (0.5 puntos)

(b) Dadas las dos funciones de codificación y decodificación del sistema RSA, muéstranos las dos funciones, una inversa de la otra. Sobre que propiedades se basa la seguridad del sistema RSA. (0.6 puntos)

(c) Siendo $N=56$, y $i=8$ los parámetros de un sistema RSA, encripta la letra "I", representada por la cifra 8. (0.4 puntos)

(d) Calcula la función de decodificación y decodifica el mensaje cifrado obtenido en el apartado anterior (0.5 puntos).

Nota: Todos los problemas puntúan por igual. No olvidéis detallar y justificar correctamente cada pregunta. Una respuesta no justificada se considerará incorrecta.