Práctica 9

Ejercicio 1 (lápiz y papel)

El siguiente sistema es tridiagonal y, como todos los sistemas tridiagonales, es muy sencillo de resolver por el método de Gauss. Resolverlo por el método de Gauss.

$$\begin{aligned} x_1 + 2x_2 &= 8 \\ 2x_1 - x_2 + x_3 &= 2 \\ x_2 + x_3 - 2x_4 &= 4 \\ 2x_3 + x_4 - x_5 &= 1 \\ x_4 + x_5 &= 1 \end{aligned}$$

Solución exacta :

$$x_1 = 2$$
$$x_2 = 3$$
$$x_3 = 1$$
$$x_4 = 0$$
$$x_5 = 1$$

Comprueba que la solución es correcta con Matlab, empleando el comando $A\backslash B$, siendo A la matriz de los coeficientes del sistema y B la matriz columna con los términos independientes.

Ejercicio 2 (ordenador)

Se trata de hacer un programa que sirva para resolver cualquier sistema tridiagonal. Para evitar la introducción de datos desde el teclado, se escribirá la matriz A de los coeficientes del sistema y B los términos independientes al comienzo del programa, pero el código debe ser general, de manera que sólo modificando A y B debe seguir funcionando correctamente. Resolver el sistema tridiagonal siguiente usando el método de Gauss:

$$\left.\begin{aligned} 4x_1 + x_2 &= 9 \\ 2x_1 + 3x_2 + x_3 &= 7 \\ x_2 + x_3 + x_4 &= 0 \\ 2x_3 + x_4 + 2x_5 &= 1 \\ 3x_4 + x_5 &= -2 \end{aligned}\right\}$$

Se debe resolver programando en Matlab, sin usar A\B.

La solución que debe obtenerse es: $x_1 = 2 \quad x_2 = 1 \quad x_3 = 0 \quad x_4 = -1 \quad x_5 = 1$

Ejercicio 3 (ordenador)

Modificar el programa anterior para resolver un sistema tridiagonal de 100 ecuaciones con 100 incógnitas del siguiente tipo:

$$\begin{pmatrix} 4 & 2 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 4 & 2 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 4 & 2 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 4 & 2 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ \vdots \\ x_{98} \\ x_{99} \\ x_{100} \end{pmatrix} = \begin{pmatrix} 1^2/10 \\ 2^2/10 \\ 3^2/10 \\ 4^2/10 \\ \vdots \\ 98^2/10 \\ 99^2/10 \\ 100^2/10 \end{pmatrix}$$

Si el ejercicio anterior lo has hecho general, éste se resolverá rápidamente.

(Sol. Por ejemplo: $x_{25} = 8.82099125$; $x_{100} = 227.564529$)

<u>Ejercicio 4 (lápiz y papel y ordenador)</u>: Temperatura de una placa de metal

Supongamos que tenemos una placa de metal cuadrada cuyos lados están sometidos a una cierta temperatura: El lado superior a 20º, el lado inferior a 30º, el lado izquierdo a 25º y el derecho a 20º. Supongamos que estas temperaturas en los lados permanecen constantes. Pues bien, el sistema tenderá, transcurrido un cierto tiempo, a un estado de equilibrio termal. La temperatura en un punto interior será el promedio de las temperaturas de sus vecinos. Se pretende averiguar las temperaturas en los puntos interiores de la placa cuando se alcance el equilibrio termal.

Discretizamos el problema situando una cuadrícula ficticia sobre la placa como aparece en la figura 1:

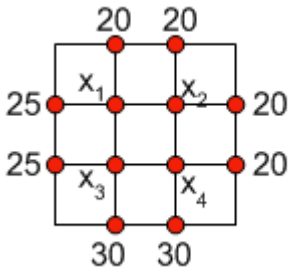

Figura 1: Discretización de una placa en 4 puntos interiores

Pues bien, en este caso hay 4 puntos interiores. La temperatura de cada uno de estos puntos será el promedio de sus 4-vecinos, por tanto:

$$x_1 = \frac{20 + 25 + x_2 + x_3}{4}$$
$$x_2 = \frac{20 + 20 + x_1 + x_4}{4}$$
$$x_3 = \frac{25 + 30 + x_1 + x_4}{4}$$
$$x_4 = \frac{20 + 30 + x_2 + x_3}{4}$$

Esto se convierte en:

$$\begin{aligned} 4x_1 - x_2 - x_3 &= 45 \\ -x_1 + 4x_2 - x_4 &= 40 \\ -x_1 + 4x_3 - x_4 &= 55 \\ -x_2 - x_3 + 4x_4 &= 50 \end{aligned}$$

Tenemos un sistema de ecuaciones lineales del tipo:

$$A = \begin{bmatrix} 4 & -1 & -1 & 0 \\ -1 & 4 & 0 & -1 \\ -1 & 0 & 4 & -1 \\ 0 & -1 & -1 & 4 \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}, \quad b = \begin{bmatrix} 45 \\ 40 \\ 55 \\ 50 \end{bmatrix}$$

Esta misma idea se puede aplicar para una cuadrícula más grande y así se obtendrán resultados más precisos. Supongamos que la cuadrícula es ahora la que viene en la figura 2 que da lugar a 25 puntos interiores. Plantear el sistema de ecuaciones y resolverlo (puedes usar la orden A\B).

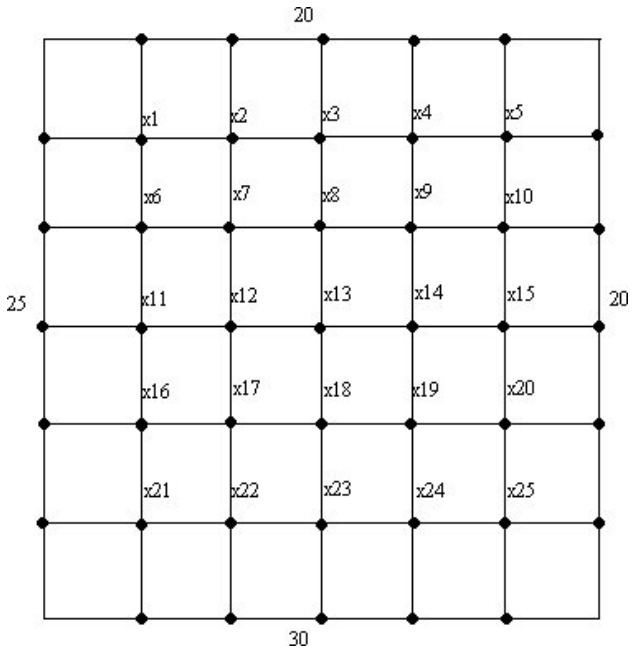

Figura 2: Discretización de una placa en 25 puntos interiores

(Sol $x_1 = 22.65, \ldots, x_{25} = 24.84$)

Ejercicio 5 (lápiz y papel): Determinantes de Vandermonde

Se llaman así a los determinantes que tienen la siguiente forma:

$\begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix}$ (determinante de Vandermonde de orden 2)

$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix}$ (determinante de Vandermonde de orden 3)

…

Comprobar que:

$$\begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = (x_2 - x_1)$$

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$$

Escribir el determinante de Vandermonde de orden 4 y calcular su valor.

Interpolación polinómica

Supongamos que trabajamos con un polinomio de segundo grado:

$$p(x) = a + bx + cx^2$$

La representación gráfica es una parábola.

Es obvio que una parábola pasa por infinitos puntos del plano.

Por ejemplo, supongamos que cogemos la parábola:

$$p(x) = x^2 + 2x + 1$$

Esta parábola pasa por lo puntos: (0, 1), (1, 4), (-1, 0), (2, 9), (3, 16), ...

Para poder determinar exactamente una parábola debemos conocer tres puntos por los que pasa

$$(x_1, y_1), (x_2, y_2), (x_3, y_3)$$

ya que tenemos tres parámetros a determinar $a, b\ y\ c$.

Si nos dan tres puntos cualesquiera de una parábola desconocida $p(x) = a + bx + cx^2$, se podrá determinar sin problemas dicha parábola ya que el sistema lineal:

$$\begin{aligned} a + bx_1 + cx_1^2 &= y_1 \\ a + bx_2 + cx_2^2 &= y_2 \\ a + bx_3 + cx_3^2 &= y_3 \end{aligned}$$

Tendrá solución única siempre que tengamos como datos tres puntos distintos de la parábola. Observa que el determinante de la matriz de los coeficientes del sistema es el determinante de Vandermonde de orden 3 que será no nulo y, por lo tanto, el sistema anterior será un sistema de Cramer y, por lo tanto, tendrá solución única.

Ejercicio 6 (lápiz y papel)

Averiguar la parábola del tipo $p(x) = a + bx + cx^2$ que pasa por lo puntos (1, 4), (-1, 0), (2, 9).

Ejercicio 7 (lápiz y papel)

Averiguar la parábola del tipo $p(x) = a + bx + cx^2$ que pasa por (1, 4), (-1, 0), (2, 9), (3, 15).

Ejercicio 8 (lápiz y papel)

Averiguar la parábola del tipo $p(x) = a + bx + cx^2$ que pasa por (1, 4), (-1, 0), (2, 9), (3, 16).

Reparto de secretos: esquema de Shamir

Existen ocasiones donde una información secreta no es deseable que esté en manos de una sola persona. Puede interesar que varias personas posean parte de dicha información y que sólo se consiga recuperar la información secreta si juntamos a varias de estas personas. Por ejemplo, una empresa puede que le interese que ningún empleado de la misma posea la clave que abre la caja fuerte. Por el contrario, puede repartir entre 6 empleados, por ejemplo, parte de la información, de forma que para conseguir la clave de la caja fuerte tengan que juntarse al menos 3 de los 6 empleados.

Este esquema se conoce con el nombre de "protocolo de Shamir", ya que fue propuesto por el criptógrafo Shamir del M.I.T. (Massachusetts Institute of Technology) en 1979 en un artículo llamado "How to share a secret". También se conoce con el nombre de esquema umbral (n,t) (se necesitan al menos t participantes de los n que hay en total para poder recuperar la clave secreta).

La idea es muy sencilla. Supongamos que $t=3$ y $n=6$. Eso quiere decir que hay 6 participantes y que sólo al juntar al menos a 3 de ellos es posible recuperar el secreto.

Supongamos que la clave secreta es $s=1234$. El distribuidor del secreto escogerá dos números cualesquiera, que indicaremos a_1 y a_2, con los que construirá el polinomio de segundo grado:

$$P(x) = s + a_1 x + a_2 x^2$$

Supongamos que $a_1 = 166$ y que $a_2 = 94$, entonces:

$$P(x) = s + a_1 x + a_2 x^2 = 1234 + 166x + 94x^2$$

Calculamos 6 puntos cualesquiera del polinomio del polinomio, por ejemplo:

(1, 1494), (3, 2578), (4, 3402), (6, 5614), (8, 8578), (11, 14434)

El distribuidor reparte aleatoriamente estos puntos entre sus seis empleados de confianza. Sólo cuando se junten al menos tres de ellos tendremos datos suficientes para poder construir el polinomio $P(x)$.

Una vez construido el polinomio será fácil recuperar el secreto s ya que: $s = P(0)$

Supongamos que al empleado nº 1 se le da el primer punto, al empleado nº 2 el segundo punto, y así en adelante.

Como el polinomio desconocido tiene 3 coeficientes a determinar hará falta un mínimo de tres puntos para poder determinarlo. Ahora bien, si se juntan tres o más sí que podrán reconstruir el polinomio.

Por ejemplo, supongamos que se juntan los empleados 2, 3, 5 y 6. El sistema a resolver sería:

$$\left.\begin{array}{l} s+3a_1+9a_2=2578 \\ s+4a_1+16a_2=3402 \\ s+8a_1+64a_2=8578 \\ s+11a_1+121a_2=14434 \end{array}\right\}$$

Comprueba con Matlab/Octave, empleando la orden rank, que $r(A) = r(A^*) = 3 =$ nº de incógnitas, por lo tanto, el sistema tiene solución única. Además, como $r(A^*) = 3$, cualesquiera tres ecuaciones nos sirven para obtener la solución del sistema (hay una ecuación redundante). Usando la orden A\B, comprueba que se obtiene la solución correcta.

La idea de Shamir es sencilla, el secreto se hace coincidir con el término independiente del polinomio y el grado del polinomio depende del número mínimo de empleados que deben juntarse para poder obtenerlo.

Para un esquema (6, 3) como el anterior, el polinomio debía ser de grado 2, para que el polinomio a determinar tenga 3 incógnitas y hagan falta como mínimo 3 puntos para poder determinarlo.

Ejercicio 9 (lápiz y papel)

Consideremos un esquema de reparto de secretos (5, 4), donde los puntos repartidos han sido:

Nº empleado	1	2	3	4	5
Punto	(-1, 5)	(1/2, 115/2)	(1, 73)	(2, 200)	(3/2, 115)

Con lápiz y papel averiguar el secreto, a través de planteamiento y la resolución de los sistemas de ecuaciones lineales correspondientes, en los siguientes casos:

a) si se juntan los empleados 1, 2, 4 y 5
b) si se juntan los empleados 2, 3, 4 y 5.

Te puedes ayudar de Matlab/Octave para resolver los sistemas.

Ejercicio 10 (ordenador)

El ejercicio anterior se puede resolver usando la interpolación polinómica de Lagrange estudiada en el primer cuatrimestre en la asignatura de Cálculo. Dado un conjunto de puntos en el plano, cuatro por ejemplo: (x_0, y_0), (x_1, y_1), (x_2, y_2), (x_3, y_3), el polinomio interpolador de Lagrange es:

$$P(x) = y_0 l_0(x) + y_1 l_1(x) + y_2 l_2(x) + y_3 l_3(x)$$

Siendo:

$$l_0(x) = \frac{(x - x_1)(x - x_2)(x - x_3)}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)}$$

$$l_1(x) = \frac{(x - x_0)(x - x_2)(x - x_3)}{(x_1 - x_0)(x_1 - x_2)(x_1 - x_3)}$$

Etc.

Haz un programa de ordenador para resolver ahora el ejercicio 9 usando ahora el método de Lagrange.

Nota: recuerda que el secreto se obtiene evaluando el polinomio interpolador en $x = 0$

Reparto de una imagen secreta

Podríamos aplicar el método de reparto de secretos de Shamir [1], estudiado anteriormente, para el reparto de una imagen digital. Sin embargo, vamos a hacer un esquema sencillo de reparto de secretos (2, 2) con otro método diferente. La imagen original se muestra a la izquierda de la figura 3 y es de tamaño 256×256.

El dueño del secreto elegirá una matriz clave K inversible módulo 256 (bastará con que tenga determinante impar) y la descompondrá en la suma de dos matrices: una K_1 formada por números aleatorios entre 0 y 255 y la otra K_2 tal que: $K = K_1 + K_2 \pmod{256}$

Supongamos que la matriz K es de orden 4, por ejemplo. Entonces, para cada bloque 4×4 de la imagen original, que indicaremos por A, haremos los siguientes cálculos:

$B_1 = K_1 A \pmod{256}$
$B_2 = K_2 A \pmod{256}$

El bloque A de la imagen original se sustituye por B_1 en la sombra 1 y por B_2 en la sombra 2. Razonando de esta forma se obtienen los resultados de la figura 5.

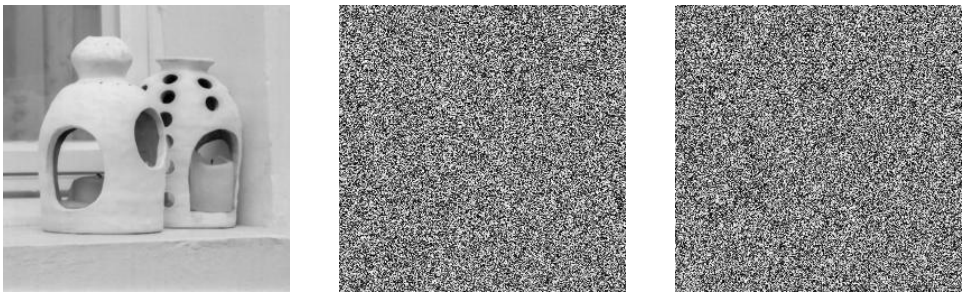

Figura 3: Imagen original y las dos sombras.

Los dos participantes conocerán la matriz K solamente y sus respectivas sombras. Cuando se junten los dos podrán recuperar la imagen secreta ya que:

$$B_1 + B_2 = K_1 A + K_2 A = (K_1 + K_2)A = K\,A \Rightarrow A = K^{-1}(B_1 + B_2) \pmod{256}$$

Ejercicio 11 (ordenador)

En Moodle encontrarás las imágenes sombra1.png y sombra2.png. Ambas imágenes son las dos sombras del esquema (2, 2) anterior aunque para otra imagen secreta. La matriz clave empleada fue:

$$K = \begin{pmatrix} 3 & 121 & 206 & 47 \\ 45 & 0 & 155 & 25 \\ 164 & 97 & 253 & 135 \\ 53 & 41 & 211 & 0 \end{pmatrix}$$

Esta matriz tiene la ventaja de ser autoinversible módulo 256, es decir, su inversa coincide con ella misma, como puedes comprobar con Matlab. Debes recuperar la imagen secreta a partir de las dos sombras.

Bibliografía

[1] Shamir, A. "How share a secret". Communications of the ACM, 22 (11), pp. 612-613, 1976.