Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática
Segundo Semestre de 2024

MAT1203L ⋆ Laboratorio Introducción al Álgebra Lineal

Laboratorio 4

Objetivos del laboratorio

- Generar matrices con valores aleatorios en Mathematica.
- Calcular inversas de matrices ocupando Mathematica.
- Mostrar una aplicación de las matrices inversas.

1. Criptografía y el uso de matrices

La criptografía es la ciencia que estudia técnicas para asegurar la comunicación y proteger la información contra el acceso no autorizado. Su objetivo principal es cifrar (o encriptar) datos para que solo las personas autorizadas puedan acceder a ellos mediante un proceso de descifrado. Las matrices juegan un papel importante en ciertos tipos de criptografía, especialmente en los sistemas de cifrado basados en álgebra lineal, como los sistemas criptográficos de matrices.

1.1. Uso de matrices en criptografía

En criptografía, las matrices se pueden utilizar para realizar cifrados y descifrados de mensajes. Una de las técnicas más comunes que utilizan matrices es el **cifrado de Hill**, un sistema de cifrado polialfabético creado por Lester S. Hill en 1929, basado en operaciones matriciales. En este método, un mensaje de texto se representa mediante una matriz numérica y luego se cifra multiplicando por otra matriz (llave).

1.1.1. Proceso de cifrado

El cifrado de Hill se basa en los siguientes pasos:

1. **Codificación del mensaje**: Se representa el mensaje de texto en una matriz de números, donde cada letra del alfabeto se convierte en un número (por ejemplo, A = 1, B = 2, ..., Z = 26). Si el mensaje no tiene un número de caracteres divisible por el tamaño de la clave (que es una matriz cuadrada), se completa el mensaje con caracteres adicionales como espacios o letras repetidas.
2. **Matriz clave**: Se elige una matriz cuadrada A, llamada *matriz clave*. Esta matriz debe tener inversa, ya que es necesaria para descifrar el mensaje. El tamaño de esta matriz determina el número de caracteres que se procesan a la vez (es decir, el tamaño del bloque).

3. **Multiplicación**: El mensaje codificado se organiza en bloques de números que forman una matriz y luego se multiplica por la matriz clave A. La operación de multiplicación genera una nueva matriz que representa el mensaje cifrado. El cifrado generalmente se realiza en aritmética modular, utilizando un módulo n, donde n es el número de letras en el alfabeto (por ejemplo, $n = 26$ para el alfabeto inglés).

4. **Mensaje cifrado**: La matriz resultante de la multiplicación es el mensaje cifrado, que luego se traduce nuevamente en letras usando la codificación del alfabeto.

1.1.2. Proceso de descifrado

Para descifrar el mensaje, se realiza el proceso inverso:

1. **Matriz inversa**: Se calcula la inversa de la matriz clave A^{-1}. Esto es posible siempre que el determinante de la matriz clave A sea distinto de cero, lo que asegura que la matriz sea invertible.

2. **Multiplicación inversa**: Se toma el mensaje cifrado (ahora en forma de matriz) y se multiplica por la matriz inversa A^{-1} para obtener el mensaje original codificado.

3. **Decodificación**: Finalmente, los números en la matriz resultante se convierten nuevamente en letras utilizando la misma tabla de codificación que en el cifrado.

1.2. Ejemplo simplificado

Consideremos un ejemplo donde usamos una matriz clave de tamaño 2×2 para cifrar y descifrar un mensaje. Supongamos que la clave es la siguiente matriz:

$$A = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Cifrado: Si el mensaje original es "HI", primero convertimos las letras en números, por ejemplo, H = 8, I = 9. El mensaje se organiza en un vector columna:

$$M = \begin{bmatrix} 8 \\ 9 \end{bmatrix}$$

Multiplicamos el vector por la matriz clave A:

$$C = A \cdot M = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 51 \\ 61 \end{bmatrix}$$

Descifrado: Para descifrar el mensaje, calculamos la inversa de la matriz clave A^{-1}, que multiplicaremos por el mensaje cifrado para recuperar el mensaje original.

1.3. Ventajas y desafíos

El uso de matrices en criptografía ofrece ciertas ventajas:

- **Procesamiento en bloques**: Las matrices permiten cifrar bloques de texto de una sola vez, lo que puede ser más eficiente que los cifrados monoalfabéticos tradicionales.
- **Mayor seguridad**: Debido a la dependencia en la estructura de la matriz clave, este tipo de cifrado es menos vulnerable a ataques que los cifrados simples como el cifrado César.

Sin embargo, uno de los principales desafíos es garantizar que la matriz clave sea invertible. Además, si el atacante logra descubrir la matriz clave o su inversa, el sistema se vuelve vulnerable.

2. Cifrado de Hill con matrices y reducción modular

Sea A una matriz invertible de tamaño $n \times n$, y M un mensaje representado como una matriz de tamaño $n \times m$. El mensaje cifrado se obtiene multiplicando la matriz del mensaje por la matriz clave A, es decir:

$$C = AM$$

Para descifrar el mensaje, basta con multiplicar el mensaje cifrado C por la matriz inversa de A, obteniendo así el mensaje original:

$$A^{-1}C = A^{-1}(AM) = IM = M$$

En este proceso, para que el resultado del cifrado permanezca dentro del rango de las letras del alfabeto, aplicamos la operación de reducción modular $\mod 27$, utilizando 27 caracteres: 26 letras del alfabeto y un carácter adicional que corresponde al espacio entre palabras.

2.1. Observación sobre el tamaño de la matriz

El tamaño de la matriz clave A no es fijo y depende de quien cifra el mensaje. En este ejemplo utilizamos una matriz de tamaño 3×3, pero podría ser de otro tamaño, como 2×2, 4×4, o más grande, dependiendo de cuántos caracteres se deseen procesar al mismo tiempo. Sin embargo, es importante que la matriz A sea invertible, lo que significa que su determinante debe ser distinto de cero.

2.2. Ejemplo de cifrado

Supongamos que el mensaje original es:

hoy es el primer dia

El primer paso es codificar el mensaje utilizando números de acuerdo a la siguiente tabla, donde el número 27 se usará para representar el espacio entre palabras:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

21	22	23	24	25	26	27
U	V	W	X	Y	Z	Espacio

Así, el mensaje queda codificado de la siguiente manera:

H	O	Y		E	S		E	L		P	R	I	M	E	R		D	I	A
8	15	25	27	5	19	27	5	12	27	16	18	9	13	5	18	27	4	9	1

2.3. Clave de cifrado

Dada la clave:

$$A = \begin{bmatrix} -1 & 1 & 1 \\ -2 & -3 & 1 \\ 3 & 1 & -2 \end{bmatrix}$$

El primer paso para cifrar el mensaje es dividirlo en grupos de tres letras, completando con espacios en blanco si es necesario, de manera que el número total de letras sea múltiplo de 3:

H	O	Y		E	S		E	L		P	R	I	M	E	R		D	I	A		
8	15	25	27	5	19	27	5	12	27	16	18	9	13	5	18	27	4	9	1	27	

2.4. Construcción de la matriz del mensaje

Luego, construimos la matriz M del mensaje, donde cada grupo de tres letras se convierte en una columna de la matriz:

$$M = \begin{bmatrix} 8 & 27 & 27 & 27 & 9 & 18 & 9 \\ 15 & 5 & 5 & 16 & 13 & 27 & 1 \\ 25 & 19 & 12 & 18 & 5 & 4 & 27 \end{bmatrix}$$

2.5. Cifrado

Para obtener el mensaje cifrado, realizamos el producto de la matriz clave A y la matriz del mensaje M.

$$C = AM = \begin{bmatrix} 32 & -3 & -10 & 7 & 9 & 13 & 19 \\ -36 & -50 & -57 & -84 & -52 & -113 & 6 \\ -11 & 48 & 62 & 61 & 30 & 73 & -26 \end{bmatrix}$$

El mensaje cifrado, escrito como matriz, es entonces:

$$\begin{bmatrix} 32 & -3 & -10 & 7 & 9 & 13 & 19 \\ -36 & -50 & -57 & -84 & -52 & -113 & 6 \\ -11 & 48 & 62 & 61 & 30 & 73 & -26 \end{bmatrix}$$

2.6. Descifrado

Para descifrar el mensaje, multiplicamos el mensaje cifrado C por la inversa de la matriz A, y nuevamente aplicamos reducción modular $\mod 27$ para obtener los valores originales:

$$M = A^{-1}C = \begin{bmatrix} 8 & 27 & 27 & 27 & 9 & 18 & 9 \\ 15 & 5 & 5 & 16 & 13 & 27 & 1 \\ 25 & 19 & 12 & 18 & 5 & 4 & 27 \end{bmatrix}$$

Esto nos devuelve el mensaje original codificado, que al decodificarlo usando la tabla de letras, obtenemos el mensaje "hoy es el primer día".

2.7. Ejercicio

Codifique el siguiente mensaje:

Si quieres saber cómo es un hombre, echa un vistazo al modo en que trata a sus inferiores, no a sus iguales

Debe crear una llave A y ocupe el 28 para la coma (,). Decodifique el siguiente mensaje:

$$\begin{bmatrix} 101 & 39 & 39 & 122 & 165 & 156 & 57 & 38 & 189 & -16 \\ -76 & -142 & -124 & 20 & 38 & 34 & -96 & -98 & -24 & -282 \\ 170 & 71 & 84 & 58 & 99 & 17 & 222 & 91 & 136 & 165 \\ -400 & -395 & -454 & -229 & -376 & -148 & -360 & -316 & -320 & -424 \\ 122 & 189 & 158 & 128 & 111 & 191 & 36 & 113 & 204 & 237 \\ 480 & 417 & 490 & 248 & 427 & 135 & 476 & 357 & 370 & 481 \end{bmatrix}$$

Donde la llave A es la matriz

$$A = \begin{bmatrix} 7 & -3 & -2 & 1 & 3 & 2 \\ 6 & -4 & -2 & -2 & -4 & 2 \\ -3 & 2 & -1 & -1 & 6 & 5 \\ -1 & -5 & -5 & -4 & -4 & -4 \\ 5 & 0 & -1 & 5 & 6 & -3 \\ -1 & 6 & 5 & 3 & 6 & 7 \end{bmatrix}$$

¿De quien es la cita?