**SECCION 1.3 AJUSTE POLINOMIAL DE CURVAS**

**EJEMPLO 4** **| Una aplicación del ajuste de curvas**

**Problema (a):** ¿Por qué en este ejemplo usan una función logarítmica para relacionar mejor el periodo de los 3 primeros planetas y su distancia media al sol, y da un mejor ajuste?

**Solución:** El problema planteado en este ejemplo se puede abordad desde un enfoque “más estadístico” para ello el concepto de regresión es útil.

En palabras propias una regresión es una relación entre dos variables (X e Y)

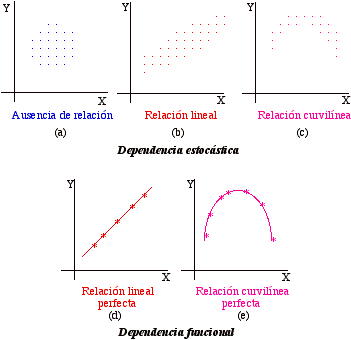
De una forma general lo primero que suele hacerse para saber si dos variables están relacionados (saber si existe regresión), (de ahora en adelante se denominaran X e Y, siendo Y la variable dependiente y X la variable independiente o regresora).

Consiste en tomar una muestra aleatoria. Sobre cada individuo de la muestra se analizan las dos características en estudio de modo que para cada individuo se tenga un par de valores.

Segundamente, se representan dichos valores en unos ejes cartesianos, dando lugar a un diagrama de dispersión o nube de puntos. Así, cada individuo vendrá representado por un punto en el gráfico de coordenadas De esa forma se podrá obtener una primera idea acerca de la forma y de la dispercion de la nube de puntos.

Sin embargo deberá distinguirse entre dependencia funcional y dependencia estocástica, en el primer caso la relación es perfecta es decir, los puntos del diagrama de dispersión correspondiente aparecen sobre la función

Sin embargo, suele ocurrir que no hay una dependencia funcional perfecta, sino otra dependencia o relación menos rigurosa o dependencia estocástica. Entonces la relación entre X e Y, se escribiría , donde es un error (o residual), debido a por ejemplo, a no incluir variables en el modelo que son importantes a la hora de explicar el comportamiento de Y, y cuyos efectos sean diferentes a los de X; errores aleatorios o de medida o simplemente que se ha especificado mal el modelo.



**Tipos de regresión:** Si las dos variables X e Y se relacionan según un modelo de línea recta se habla de relación lineal simple

Cuando las variables X e Y se relacionan según una línea curva se habla de regresión no lineal o curvilínea. Aquí se puede distinguir entre regresión parabólica, exponencial, potencial, etc.

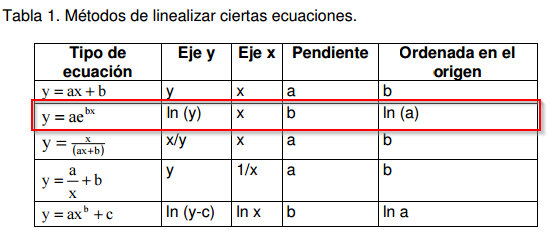
Cuando hay más de una variable independiente y una sola variable dependiente Y, se habla de regresión múltiple. Las variables se denominan regresoras, predictoras o independientes.

**Causalidad:** Es muy importante resaltar el hecho, de que un modelo sea capaz de explicar de manera adecuada las variaciones de la variable dependiente en función de la variable independiente, no implica que la primera sea causa de la segunda.

Es un error muy común confundir causalidad con casualidad. El hecho de que dos variables estén relacionadas no implica que una sea causa de la otra. Por ejemplo, si se realiza un estudio en el que se analizó el número de canas (X) y la presión arterial (Y) podría encontrarse una relación lineal casi perfecta. Eso no significa que el tener canas aumente la presión arterial, lo que verdaderamente está ocurriendo es que es la edad la causante de que se tengan más canas y una tendencia a tener más alta la presión arterial.

**Linealización:** Algunos problemas de regresión no lineal pueden linealizarse mediante una transformación en la formulación del modelo. Por ejemplo, considere el problema de regresión no lineal (ignorando el término del error)

Aplicando logaritmos a ambos lados de la expresión se obtiene:



**Aplicando lo anterior al ejemplo:**

Dados los datos en originales, procedemos sacando logaritmo natural a las variables de las muestras x e y. obteniendo la siguiente tabla.

|  |  |  |
| --- | --- | --- |
|  | Distancia media al sol (Ln(x)) | Periodo (Ln(y)) |
| Mercurio | **-0.949** | **-1.423** |
| Venus | **-0.324** | **-0.486** |
| Tierra | **0** | **0** |
| Marte | **0.421** | **0.632** |
| Júpiter | **1.649** | **2.473** |
| Saturno | **2.256** | **3.383** |

Al aplicar este método de Linealización efectivamente, podemos observar que obtenemos una línea recta, se sabe que la ecuación de una línea en esta dada por: , donde m es la pendiente y b la ordenada en el origen (Punto en el que la línea corta al eje y)

Si:

Tomando los valores x, y de marte y la tierra para hallar la pendiente de la línea.

Luego la ecuación de la línea queda:

Así, se puede decir que el cuadrado del periodo de los planetas es igual al cubo de su distancia media al sol.

**Referencias Bibliográficas:**

#### Pedimos disculpas, la gran parte de este texto esta sacado de una artículo de internet cuya URL hemos perdido.

(2016). [online] Available at: <http://goo.gl/sxYxYb> [Accessed 8 Apr. 2016].

#### (2016). *Rua.ua.es*. Retrieved 8 April 2016, from <http://goo.gl/Ahnf60>

**SECCION 2.4 MATRICES ELEMENTALES**

**EJEMPLO 5A** **| Factorización LU**

**Problema (a):** Demuestre la siguiente factorización LU

A =

**Solución:** Para hallar la matriz L y la matriz U debemos seguir los siguientes procedimientos

**Primero:** Aplicando solo operaciones elementales de suma y resta entre renglones debemos intentar expresar la matiz como una matriz equivalente escalonada por renglones.

**Segundo:** Cada operación que realicemos en los renglones de deberá ser almacenada en una matriz elemental de tal forma que , Donde sea el producto de matrices elementales que almacenan las operaciones elementales realizadas en los renglones de , y sea la matriz escalonada por renglones.

|  |  |
| --- | --- |
| OPERACIÓN ELEMENTAL | MATRIZ ELEMENTAL |
|  |  |

Así la situación está de la siguiente manera:

Observemos que en la matriz ya es escalonada por renglones (triangular superior), es decir y , de esta manera podemos decir que

**SECCION 2.5 CRIPTOGRAFIA**

Un criptograma es un mensaje escrito de acuerdo con un código secreto.

En el campo de la criptografía muchas veces se agrupan conjuntos de funcionalidades que tienen una característica común y ese conjunto lo denominan “criptografía de [la característica que comparten]”, Ejemplos:

* Criptografía simétrica
* Criptografía asimétrica o de clave publica
* Criptografía hibrida

**Criptografía simétrica:** o criptografía de una clave (en inglés single-key cryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo.

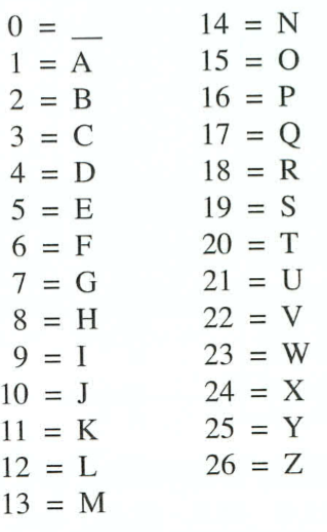
Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio/distribución de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

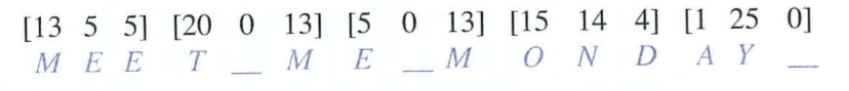
Basado en lo anterior, podemos decir que los ejemplos descritos a continuación usan un método criptográfico simétrico, además estos ejemplos describen uno de muchos posibles algoritmos de encriptación, es decir, este algoritmo no es ni el único, ni el mejor.

**EJEMPLO 4** **| Formación de matrices sin codificar**

Empecemos por asignar un número a cada letra del alfabeto:

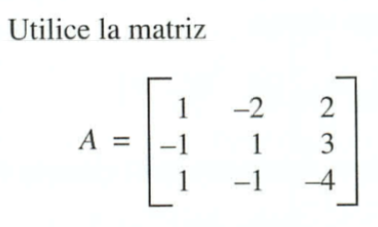


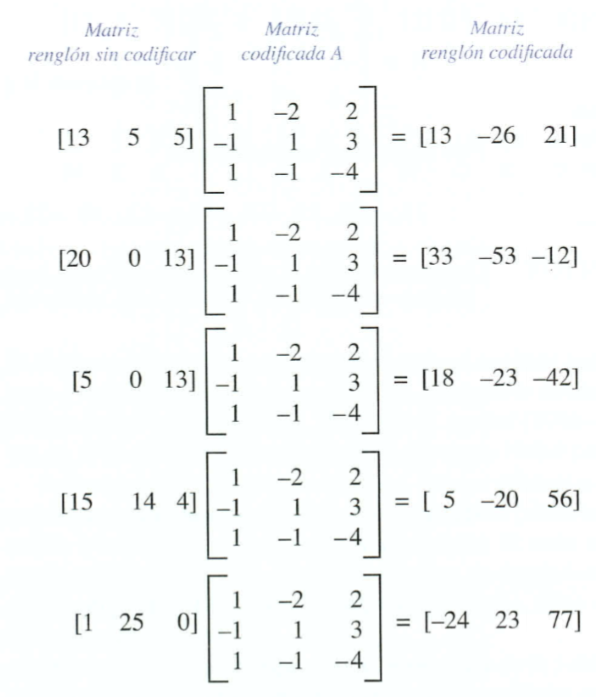
Supongamos que queremos codificar el mensaje MEET ME MONDAY, debemos dividir el mensaje en matrices renglón conveniente. Ejemplo dividámosla en matrices renglón de 1x3



**EJEMPLO 5** **| Codificación de un mensaje**

Ahora debemos buscar una matriz invertible de orden nxn y multiplicarla por las matrices renglón sin codificar (por la derecha)





Nota: Si la matriz renglón sin codificar es de orden 1xn, y la matriz codificada es de orden nxn, la matriz codificada se debe multiplicar por la derecha de la matriz renglón sin codificar porque la multiplicación de matrices no está definida, pues el número de columnas de A es diferente al número de renglones de B.

**EJEMPLO 6** **| Decodificación de un mensaje**

Si es una matriz de 1xn sin codificar, entonces es la matriz codificada correspondiente donde A es una matriz cuadrada de orden n e invertible.

El receptor de la matriz codificada puede decodificar Y multiplicando el lado derecho por para obtener:

Se sabe que una de las propiedades de la matriz inversa es:

Y también se sabe que para matrices cuadradas:

**Bibliografía:**

#### *Criptografía*. (2016). *Es.wikipedia.org*. Retrieved 8 April 2016, from <https://goo.gl/FGUgnS>

#### *Criptografía simétrica*. (2016).*Es.wikipedia.org*. Retrieved 8 April 2016, from <https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica>

**SECCION 4.7 COORDENADAS Y CAMBIO DE BASE**

**EJEMPLO 1** **| Coordenadas y componentes en**

**Problema de coordenadas y componentes en :** Determinar la matriz de coordenadas de en con respecto a la base estándar

**Solución:** Se sabe que la matriz de coordenadas del vector con respecto a la base estándar esta determinada por los coeficientes que resultan de la combinación lineal de que forman el vector , esto es.

Sea entonces

De esta manera sabemos que los valores que descubramos para van a ser las coordenadas del vector con respecto a . Y se denotaran como (véase que el subíndice de la anterior notación indica con respecto a que base esta la coordenada del vector dado), si intentamos solucionar el problema vamos a obtener que

Entonces como , son los coeficientes de la combinación lineal de que forman al vector , podemos afirmar que . Así las componentes del vector son las mismas que sus coordenadas con respecto a la base estándar .

**EJEMPLO 2** **| Matriz de coordenadas con respecto a base estándar**

**Problema de determinación de una matriz de coordenadas con respecto a una base estándar:** La matriz de coordenadas del vector en con respecto a la base no estándar es , determine las coordenadas de con respecto a la base estándar

**Solución:** Dado que son las coordenadas de un vector con respecto a la base no estándar es correcto afirmar que:

Así es la coordenada del vector con respecto a la base no estándar . El problema ahora es determinar las coordenadas del vector

De esta manera la coordenada del vector con respecto a la base estandar es

**EJEMPLO 3** **| Matriz de coordenadas con respecto a base no estándar**

**Problema de determinación de una matriz de coordenadas con respecto a una base no estándar:** Encuentre la matriz de coordenadas del vector en con respecto a la base no estándar

**Solución:** Se sabe que las componentes de la matriz de coordenadas de con respecto a la base no estándar están determinadas por los coeficientes de la combinación lineal de que forman al vector . Así, podemos afirmar que:

Al igualar las componentes se obtiene el siguiente sistema de ecuaciones lineales y la siguiente ecuación matricial.

Procedemos ahora a resolver el sistema aplicando **gauss** o **gauss-jordan** a la matriz aumentada que se obtuvo del sistema anterior.

|  |  |
| --- | --- |
| OPERACIÓN ELEMENTAL | RESULTADO EN MATRIZ |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Entonces , Asi

Por tanto decimos que la coordenada del vector con respecto a la base es el vector