

INFORMÁTICA TEÓRICA
Ingeniería Superior Informática
Curso 2007/2008. Septiembre
Práctica de Máquinas de Turing

La práctica consiste en diseñar una máquina de Turing capaz de codificar mensajes mediante el procedimiento dado.

Cifrado César

En criptografía, un cifrado César, también conocido como cifrado por desplazamiento, es una de las técnicas de codificación más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra en una posición que está un número determinado de espacios más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería reemplazada por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etcétera. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales. Por ejemplo, un cifrado César con desplazamiento 2 transformaría las letras de esta forma:

A → C
B → D
C → E
D → F
E → G
...
X → Z
Y → A
Z → B

Y el mensaje “HOLA” quedaría transformado en “JQNC”

Cifrado para la práctica

El cifrado usado en la práctica será una variante del cifrado César. Por un lado se separarán las letras del abecedario en tres conjuntos distintos, y se usará los desplazamientos dados como parámetros sobre cada uno de ellos.

El primer conjunto estará formado por los caracteres: A, B, C, D, E, F, G

El segundo conjunto estará formado por los caracteres: H, I, J, K, L, M, N, O, P

El tercer conjunto estará formado por los caracteres: Q, R, S, T, U, V, W, X, Y, Z

Por ejemplo una codificación (3,2,-1) significará un desplazamiento 3 sobre el primer conjunto, y 2 sobre el segundo, y -1 sobre el tercero, de forma que:

Conjunto 1	Conjunto 2	Conjunto 3
A → D	H → J	Q → Z
B → E	I → K	R → Q
C → F	J → L	S → R
D → G	K → M	T → S
E → A	L → N	U → T
F → B	M → O	V → U
G → C	N → P	W → V
	O → H	X → W
	P → I	Y → X
		Z → Y

A la hora de ejecutar la máquina de Turing, que se llamará **codifica**, la cinta de entrada contendrá los desplazamientos de cada grupo de letras entre paréntesis y separados por una coma, y a continuación el mensaje a codificar (en caracteres con mayúsculas):

Ejemplo:

Cinta inicial:(3,2,-1)HOLA.....

El estado final de la cinta debe ser igual que el inicial, pero añadiendo al final del mensaje a codificar un carácter “=” y la codificación del mensaje. El resto de la cinta deberá estar vacía.

Ejemplo:

Cinta inicial:(3,2,-1)HOLA.....

Cinta final:(3,2,-1)HOLA=JHND.....

Comentarios:

- No está permitido el uso del desplazamiento nulo (N) de la cabeza lectora.
- Los desplazamientos serán número enteros, aunque pueden ser 0, números de más de una cifra e incluso negativos.

Ejemplo:

Cinta final:(100,2,0)HOLA=JHNC.....

- El estado final de la cinta deberá ser un estado llamado “fin” declarado como final, y la cabeza lectora deberá estar posicionada al final del texto de la cinta:

Cinta final:(100,2,0)HOLA=JHNC <fin>.....

- En el contenido inicial de la cinta no habrá ningún carácter no contemplado (Ñ,<,\$,... etc), así como un formato no válido para los números (010, --14, +128, ...etc). Por tanto, las máquinas de Turing no deberán preocuparse de verificar el formato del contenido inicial de la cinta.

Se debe entregar:

1. **Memoria** en papel con los siguientes apartados:

- Portada (1 hoja). Nombre y **dirección de correo electrónico activo** de los alumnos
- Índice (1 hoja).
- Introducción (máximo 1 hoja).
- Breve descripción del algoritmo (máximo 1 hoja).
- Diseño de la máquina de Turing y explicación del funcionamiento, dando una visión global de la funcionalidad de sus estados.
- Tres ejemplos, como mínimo, de funcionamiento. Uno de los ejemplos debe ser el indicado en el enunciado: “(3,2,-1)HOLA”
- Conclusiones (máximo 1 hoja).
- La memoria no debe ser superior a 30 folios.

2. **Por email** se enviará un fichero ZIP con los siguientes ficheros:

- `codifica<NIA>.tm`: descripciones de la máquina de Turing diseñada, en el formato del simulador de la asignatura. Hay que sustituir <NIA> por el NIA de uno de los miembros del grupo.

Ejemplo: `codifica100014840.tm`

Dicho fichero sólo contendrá la descripción de la máquina. No deberá contener **ninguna ejecución** de la máquina.

- `Resultado1.sal`, `Resultado2.sal`, `Resultado3.sal`: ficheros de salida obtenidos para el primer, segundo y tercer ejemplo. Esta salida se deberá obtener con la opción ‘- q’ del simulador.

Este fichero ZIP se enviará al profesor de prácticas (cluque@inf.uc3m.es en Leganés y fcastane@inf.uc3m.es en Colmenarejo) con asunto “IT2 – Práctica Turing – NIA” donde NIA se sustituirá por el NIA usado en el nombre de la máquina de Turing.

Para aprobar la práctica será indispensable:

- Que la memoria sea completa y cumpla todos los requisitos especificados anteriormente.
- Que la Máquina de Turing funcione correctamente.

Los grupos de prácticas son de, como máximo, dos personas. La fecha límite de entrega de la práctica es el **día del examen de la asignatura**. Sólo se hará evaluación presencial de aquellas prácticas para cuya corrección sea deseable aclarar algún punto concreto, a juicio de los profesores de la asignatura. En tal caso, se citará a los alumnos mediante correo electrónico.

Importante

Es importante cumplir con los requerimientos establecidos en el enunciado. Hay que **respetar los nombres de las máquinas de turing** (codifica). También hay que respetar el **nombre de los archivos**.