Incertidumbre en IA

Examen de evaluación continua, Curso 2014-15

Grado en Ingeniería Informática

Inteligencia Artificial
Departamento de Informática

Universidad Carlos III de Madrid

Ejercicio 1: Redes Bayesianas

Un producto de seguridad informática debe detectar si un sistema está infectado. Esto se puede hacer reconociendo comportamientos anómalos en la carga diaria de los procesadores (que puede ser Baja o Alta) y en el tráfico diario de red (que puede ser Normal o Intenso).

Se ha medido que, si un día se produce un backup del sistema, la carga del procesador es Alta en un 75 % de los casos; cuando NO se produce, se ha medido que los sistemas infectados tienen carga alta en un 50 % de los casos, mientras que los no infectados sólo en un 25 % de los casos.

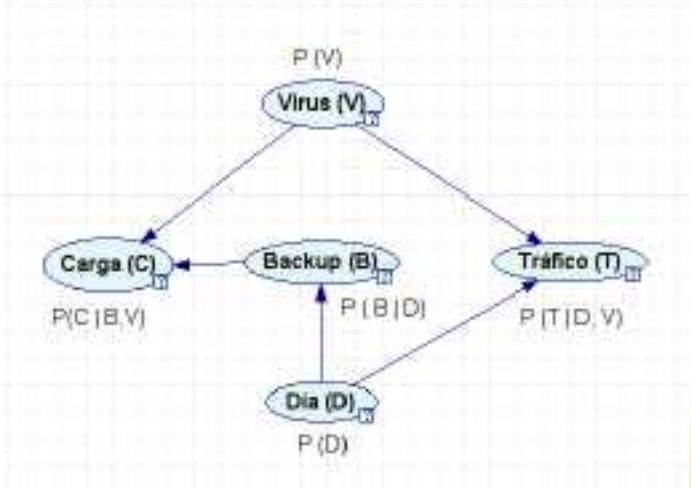
Por otro lado, en días festivos el tráfico de red es Normal el 90 % del tiempo, salvo en sistemas infectados, en los que el tráfico es Intenso el 25 % del tiempo. En días laborables, el tráfico es Intenso el 75 % del tiempo, independientemente de otros factores. En día festivo la probabilidad de que se realice un backup es del 80 % y sólo del 40 % en día laborable.

1. Modelar el problema anterior mediante una técnica probabilística de las vistas en clase, sabiendo que uno de cada cuatro días es festivo en este país y que la incidencia general de virus es del 1 %. Indicar con claridad a qué probabilidades nos referimos con cada una de las cifras del enunciado.
2. Calcular qué probabilidad dará el sistema de que haya virus, si se detecta Carga Alta y Tráfico Intenso en un día Festivo. Escriba las expresiones primero "indicadas" en función de las probabilidades, y luego sustituya por los valores tomados del modelo anterior

Ejercicio 1: Solución

La técnica son Redes Bayesianas, no necesariamente temporales. Se describe un sistema de diagnóstico (de si hay o no virus) a partir de ciertas variables que son causadas (parcialmente) por este hecho. Las relaciones de causalidad entre variables son las que se indican en la figura.

Virus (V)	$\in \{v, \neg v\}$
	v (true) significa que hay virus
Día (V)	$\in \{d, f\}$
	f significa que el día es festivo
Backup (B)	$\in \{b, \neg b\}$
	b significa que hubo backup
Carga (C)	$\in \{baja, alta\}$
Tráfico (T)	$\in \{normal, intenso\}$



Ejercicio 1: Solución (CPT's)

Las probabilidades del enunciado son las que identificamos en las siguientes tablas.

P(V)	V=v	V=$\neg v$
	0.01	0.99

P(D)	D=d	D=$\neg f$
	0.75	0.25

P(B | D)	B=b	B=$\neg b$
D=d	0.4	0.6
D=f	0.8	0.2

P(C | B,V)		C=*baja*	C=*alta*
B=b	V=v	0.25	0.75
B=b	V=$\neg v$	0.25	0.75
B=$\neg b$	V=v	0.5	0.5
B=$\neg b$	V=$\neg v$	0.75	0.25

P(T | D,V)		T=*normal*	T=*intenso*
D=d	V=v	0.25	0.75
D=d	V=$\neg v$	0.25	0.75
D=f	V=v	0.75	0.25
D=f	V=$\neg v$	0.90	0.10

Ejercicio 1: Solución (Inferencia)

Calcular qué probabilidad dará el sistema de que haya virus, si se detecta Carga Alta y Tráfico Intenso en un día Festivo.

- Hay que calcular, por un lado, $P(v|C = alta, T = intenso, D = f)$, y por otro $P(\neg v|C = alta, T = intenso, D = f)$

$$
\begin{aligned}
&P(v|C = alta, T = int, D = f) = \alpha \cdot P(v, C = alta, T = int, D = f) \\
&= \alpha \cdot \sum_{B} P(v, C = alta, T = int, D = f) \\
&= \alpha \cdot \sum_{B=b_i} P(v) \cdot P(D = f) \cdot P(B = b_i|D = f) \cdot P(T = int|D = f, v) \cdot P(C = alta|B = b_i, v) \\
&= \alpha \cdot \sum_{B=b_i} P(v) \cdot P(D = f) \cdot P(B = b_i|D = f) \cdot P(T = int|D = f, v) \cdot P(C = alta|B = b_i, v) \\
&= \alpha \cdot P(v) \cdot P(D = f) \cdot P(T = int|D = f, v) \cdot \sum_{B=b_i} P(B = b_i|D = f) \cdot P(C = alta|B = b_i, v) \\
&= \alpha \cdot P(v) \cdot P(D = f) \cdot P(T = int|D = f, v) \cdot \\
&\cdot (P(B = b|D = f) \cdot P(C = alta|B = b, v) + P(B = \neg b|D = f) \cdot P(C = alta|B = \neg b, v) \\
&= \alpha \cdot 0.01 \cdot 1.0 \cdot 0.25 \cdot (0.8 \cdot 0.75 + 0.2 \cdot 0.5) = 0.00175
\end{aligned}
$$

Ejercicio 1: Solución (Inferencia)

Calcular qué probabilidad dará el sistema de que haya virus, si se detecta Carga Alta y Tráfico Intenso en un día Festivo.

- Hay que calcular, por un lado, $P(v|C = alta, T = intenso, D = f)$, y por otro $P(\neg v|C = alta, T = intenso, D = f)$

$$
\begin{aligned}
&P(\neg v|C = alta, T = int, D = f) = \alpha \cdot P(\neg v, C = alta, T = int, D = f) \\
&= \alpha \cdot \sum_{B} P(\neg v, C = alta, T = int, D = f) \\
&= \alpha \cdot \sum_{B=b_i} P(\neg v) \cdot P(D = f) \cdot P(B = b_i|D = f) \cdot P(T = int|D = f, \neg v) \cdot P(C = alta|B = b_i, \neg v) \\
&= \alpha \cdot \sum_{B=b_i} P(\neg v) \cdot P(D = f) \cdot P(B = b_i|D = f) \cdot P(T = int|D = f, \neg v) \cdot P(C = alta|B = b_i, \neg v) \\
&= \alpha \cdot P(\neg v) \cdot P(D = f) \cdot P(T = int|D = f, \neg v) \cdot \sum_{B=b_i} P(B = b_i|D = f) \cdot P(C = alta|B = b_i, \neg v) \\
&= \alpha \cdot P(\neg v) \cdot P(D = f) \cdot P(T = int|D = f, \neg v) \cdot \\
&\cdot (P(B = b|D = f) \cdot P(C = alta|B = b, \neg v) + P(B = \neg b|D = f) \cdot P(C = alta|B = \neg b, \neg v) \\
&= \alpha \cdot 0.99 \cdot 1.0 \cdot 0.10 \cdot (0.8 \cdot 0.75 + 0.2 \cdot 0.25) = 0.06435
\end{aligned}
$$

Ejercicio 1: Solución (Inferencia)

Calcular qué probabilidad dará el sistema de que haya virus, si se detecta Carga Alta y Tráfico Intenso en un día Festivo.

- Ahora basta normalizar

$$P(v|C = alta, T = int, D = f) = \alpha \cdot 0.01 \cdot 1.0 \cdot 0.25 \cdot (0.8 \cdot 0.75 + 0.2 \cdot 0.5) = 0.00175$$
$$P(\neg v|C = alta, T = int, D = f) = \alpha \cdot 0.99 \cdot 1.0 \cdot 0.10 \cdot (0.8 \cdot 0.75 + 0.2 \cdot 0.25) = 0.06435$$
$$P(v|C = alta, T = int, D = f) = \frac{0.00175}{0.00175 + 0.06435} = 0.0265\ (2.65\,\%)$$

Ejercicio 2: Procesos de Decisión de Markov

En el caso anterior el sistema inteligente de gestión ha detectado un virus. En este caso debe decidir qué hacer, con la intención de identificar el virus concreto y eliminarlo en el menor tiempo posible.

Una posibilidad es ejecutar un antivirus, operación que tarda 10 min en ejecutarse. Cada pasada del antivirus sobre un virus no identificado tiene una probabilidad del 20 % de eliminarlo (E) y un 30 % de identificar el tipo de virus (I) pero no eliminarlo. Si se ejecuta cuando el virus está identificado, sigue teniendo el 20 % de eliminarlo.

Otra posibilidad es llamar al informático, que tarda 25 min en realizar su tarea. En este caso, si el virus está identificado, lo elimina con un 70 % de probabilidad. Si no lo está, lo elimina sólo con un 10 % , y lo identifica con un 70 %.

1. Representa el problema con un MDP, especificando claramente estados, transiciones, costes, y a qué probabilidades corresponden cada uno de los datos anteriores.
2. Escribir las ecuaciones de Bellman para cada estado. Primero hacerlo dejándolas indicadas, y luego sustituye para que queden ecuaciones numéricas más sencillas.
3. Realizar dos iteraciones del algoritmo de Iteración de Valores (además de la inicialización de los valores a cero).
4. Al cabo de un número suficiente de iteraciones, tenemos que el valor para el estado inicial (D) es 41 y para el estado Identificado (I) es 35. ¿Cuánto tiempo se estima que se tardará en resolver la incidencia? Determine cuál es la política óptima en cada uno de los estados.

Ejercicio 2: Solución (Representación)

- Estados: D (detectado, pero no identificado), I (identificado), E (eliminado)
- Acciones: AV (pasar antivirus, coste 10) y INF (llamar informático, coste 25)
- Transiciones:

Acción: AV

	$P_{AV}(S_{t+1}\|S_t)$		
S_t	$S_{t+1} = D$	$S_{t+1} = I$	$S_{t+1} = E$
$S = D$	0.5	0.3	0.2
$S = I$		0.8	0.2

Acción: INF

	$P_{INF}(S_{t+1}\|S_t)$		
S_t	$S_{t+1} = D$	$S_{t+1} = I$	$S_{t+1} = E$
$S = D$	0.2	0.7	0.1
$S = I$		0.3	0.7

Ejercicio 2: Solución (Ecuaciones de Bellman)

Para el estado D, su valor V(D) se calcula:

$$
\begin{aligned}
V_{t+1}(D) = \text{mín}\{ & C(AV) + P_{AV}(S_{t+1} = D|S_t = D) \cdot V_t(D) + P_{AV}(S_{t+1} = I|S_t = D) \cdot V_t(I) + P_{AV}(S_{t+1} = E|S_t = D) \cdot V_t(E), \\
& C(INF) + P_{INF}(S_{t+1} = D|S_t = D) \cdot V_t(D) + P_{INF}(S_{t+1} = I|S_t = D) \cdot V_t(I) + P_{INF}(S_{t+1} = E|S_t = D) \cdot V_t(E)\} \\
V_{t+1}(D) = \text{mín}\{ & 10 + 0.50 \cdot V_t(D) + 0.30 \cdot V_t(I) + 0.20 \cdot V_t(E), \\
& 25 + 0.20 \cdot V_t(D) + 0.70 \cdot V_t(I) + 0.10 \cdot V_t(E)\} \\
V_{t+1}(D) = \text{mín}\{ & 10 + 0.50 \cdot V_t(D) + 0.30 \cdot V_t(I), \\
& 25 + 0.20 \cdot V_t(D) + 0.70 \cdot V_t(I)\}
\end{aligned}
$$

Para el estado I, su valor V(I) se calcula:

$$
\begin{aligned}
V_{t+1}(I) = \text{mín}\{ & C(AV) + P_{AV}(S_{t+1} = D|S_t = I) \cdot V(NI) + P_{AV}(S_{t+1} = I|S_t = I) \cdot V(I) + P_{AV}(S_{t+1} = E|S_t = I) \cdot V(E), \\
& C(INF) + P_{INF}(S_{t+1} = D|S_t = I) \cdot V(NI) + P_{INF}(S_{t+1} = I|S_t = I) \cdot V(I) + P_{INF}(S_{t+1} = E|S_t = I) \cdot V(E)\} \\
V_{t+1}(I) = \text{mín}\{ & 10 + 0.00 \cdot V(D) + 0.80 \cdot V(I) + 0.20 \cdot V(E), \\
& 25 + 0.00 \cdot V(D) + 0.30 \cdot V(I) + 0.70 \cdot V(E)\} \\
V_{t+1}(I) = \text{mín}\{ & 10 + 0.80 \cdot V(I), \\
& 25 + 0.30 \cdot V(I)\}
\end{aligned}
$$

Ejercicio 2: Solución (Iteración de valores)

- En la figura vemos el resultado de aplicar las ecuaciones anteriores sucesivamente.

	Detectado (D)			*Identificado (I)*		
Iteración	**Acción: AV**	**Acción: INF**	**Min**	**Acción: AV**	**Acción: INF**	**Min**
0	0	0	0	0	0	0
1	10	25	10	10	25	10
2	18	34	18	18	28	18
3	24.4	41.2	24.4	24.4	30.4	24.4
4	29.52	46.96	29.52	29.52	32.32	29.52
5	33.62	51.57	33.62	33.62	33.86	33.62
6	36.89	55.25	36.89	36.89	35.08	35.08
7	38.97	56.94	38.97	38.07	35.53	35.53
8	40.14	57.66	40.14	38.42	35.66	35.66
9	40.77	57.99	40.77	38.53	35.7	35.7
10	41.09	58.14	41.09	38.56	35.71	35.71
11	41.26	58.22	41.26	38.57	35.71	35.71
12	41.34	58.25	41.34	38.57	35.71	35.71
13	41.39	58.27	41.39	38.57	35.71	35.71
14	41.41	58.28	41.41	38.57	35.71	35.71
15	41.42	58.28	41.42	38.57	35.71	35.71
16	41.42	58.28	41.42	38.57	35.71	35.71
17	41.43	58.28	41.43	38.57	35.71	35.71
18	41.43	58.29	41.43	38.57	35.71	35.71

DATO			**41**			**35**
TEST	41	57.7	41	38	35.5	35.5
POLÍTICA	**Acción: Antivirus**			**Acción: Informático**		

Ejercicio 2: Solución (Política Óptima)

- El tiempo esperado para resolver la incidencia es el valor del estado inicial, es decir: $V_{t+1}(D) = 41$.
- Para la política en un estado, reemplazamos los valores que nos dan como dato en la ecuación del valor de dicho estado, y decidimos por la acción que da menor coste; resulta ser $\pi^*(D) = AV$, y $\pi^*(I) = INF$
- Para el estado D:

$$\begin{aligned}
\pi^*(D) = argmin_{(AV,INF)}\{&10 + 0.50 \cdot V_t(D) + 0.30 \cdot V_t(I) && (\mathbf{AV}),\\
&25 + 0.20 \cdot V_t(D) + 0.70 \cdot V_t(I) && (\mathbf{INF})\}\\
\pi^*(D) = argmin_{(AV,INF)}\{&10 + 0.50 \cdot 41 + 0.30 \cdot 35 && (\mathbf{AV}),\\
&25 + 0.20 \cdot 41 + 0.70 \cdot 35) && (\mathbf{INF})\}\\
\pi^*(D) = argmin_{(AV,INF)}\{&41, 57.4\} && = \mathbf{AV}
\end{aligned}$$

- Para el estado I:

$$\begin{aligned}
\pi^*(I) = argmin_{(AV,INF)}\{&10 + 0.80 \cdot V(I) && (\mathbf{AV}),\\
&25 + 0.30 \cdot V(I) && (\mathbf{INF})\}\\
\pi^*(I) = argmin_{(AV,INF)}\{&10 + 0.80 \cdot 35 && (\mathbf{AV}),\\
&25 + 0.30 \cdot 35 && (\mathbf{INF})\}\\
\pi^*(I) = argmin_{(AV,INF)}\{&38, 35.5\} && = \mathbf{INF}
\end{aligned}$$

Ejercicio 3: Lógica Borrosa

Un agente web va a generar una lista de viajes para un cliente. El sistema obtiene un nivel de recomendación que depende de las características del viaje y preferencias del cliente. Todas las variables se representan internamente en lógica borrosa, ya que finalmente nos basta con saber ordenar los viajes por valor de recomendación.

El experto ha decidido que se deben usar las siguientes reglas, donde la edad se define con tres términos (joven-adulto-maduro en orden creciente) y la duración del viaje con otros tres (corto-medio-largo).

R1: SI el cliente es Joven OR el viaje es de duración Media,
ENTONCES la recomendación es Recomendado

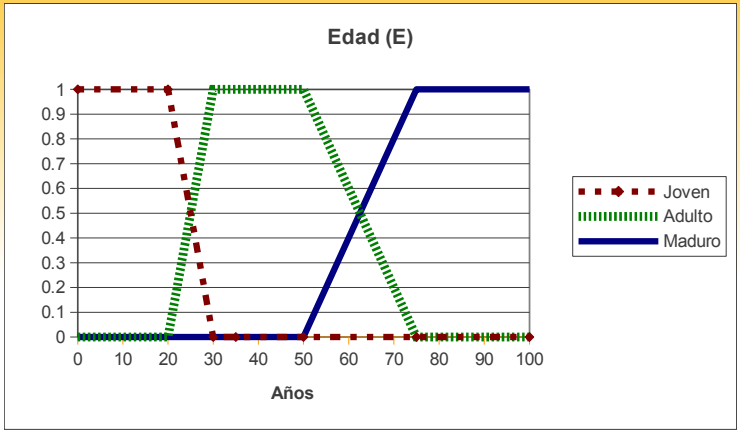
R2: SI el cliente es Maduro AND el viaje es Largo,
ENTONCES la recomendación es Desaconsejado

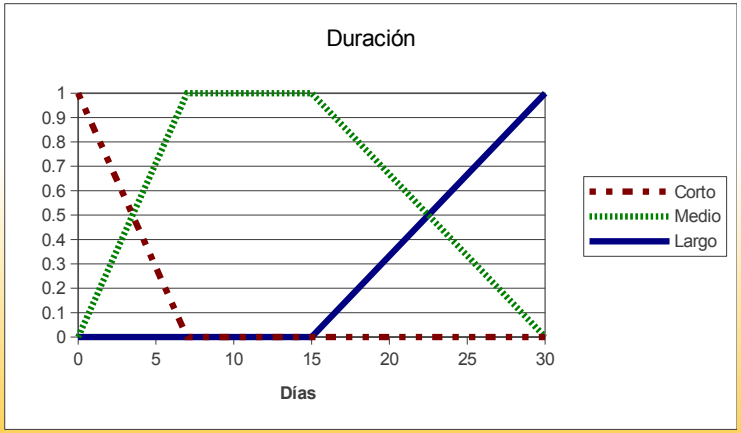
R3: SI el cliente es Adulto AND el viaje es Corto OR Largo,
ENTONCES la recomendación es Desaconsejado

Para tratar la borrosificación y deborrosificación se usan las variables y conjuntos borrosos definidos en las figuras.

1. Realizar la inferencia de tipo Mamdani para una consulta de un usuario que tiene 40 años de edad y pide un viaje de 20 días de duración.
2. Suponga que se muestran al usuario solamente viajes cuyo valor de recomendación, deborrosificado, excede 50. ¿Este viaje se le mostraría?

Ejercicio 3: Solución (Borrosificación)





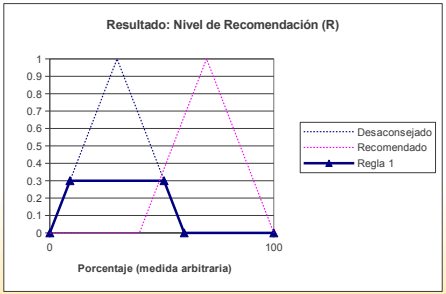
Consultando las figuras, obtenemos los valores de entrada siguientes:

- Para Edad=40 años, vemos que $\mu_{Joven} = \mu_{Maduro} = 0.0$, y $\mu_{Adulto} = 1.0$
- Para Viaje=20 días, vemos que $\mu_{Corto} = 0.0$, $\mu_{Medio} = 0.7$ y $\mu_{Largo} = 0.3$

Ejercicio 3: Solución (Reglas)

Aplicamos cada una de las reglas con los niveles de similitud que proceden de la borrosificación, y combinamos los valores usando el mínimo para el AND, y el máximo para el OR.

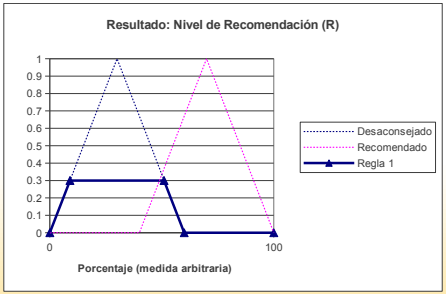
R1:	SI	el cliente es	Joven	OR	el viaje es de duración Media,
		$\mu_{Joven} = 0$		**MAX**	$\mu_{Media} = 0.7$
	$\rightarrow$	la recomendación es			Recomendado
					$\mu_{Recomendado} = MAX(0.0, 0.7) = 0.7$

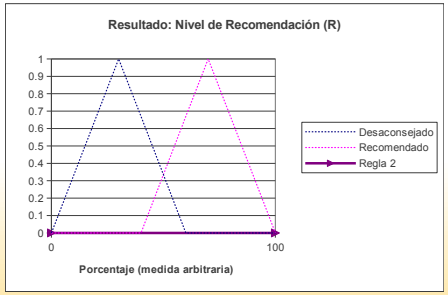


Ejercicio 3: Solución (Reglas)

Aplicamos cada una de las reglas con los niveles de similitud que proceden de la borrosificación, y combinamos los valores usando el mínimo para el AND, y el máximo para el OR.

R2:	SI	el cliente es	Maduro	AND	el viaje es Largo,
		$\mu_{Maduro} = 0$		**MIN**	$\mu_{Largo} = 0.3$
	$\rightarrow$	la recomendación es	Desaconsejado		
			$\mu_{Desconsejado} = MIN(0.0, 0.3) = 0.0$		

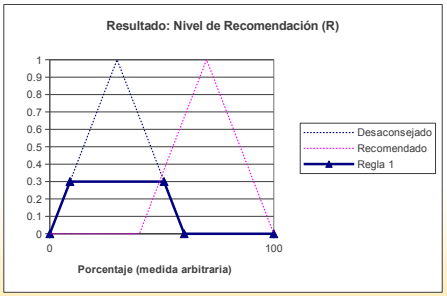


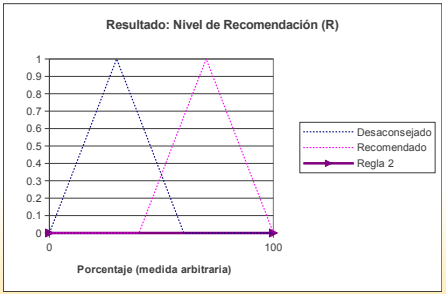


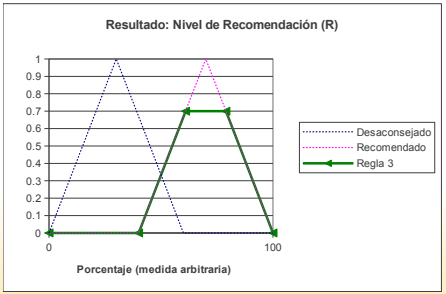
Ejercicio 3: Solución (Reglas)

Aplicamos cada una de las reglas con los niveles de similitud que proceden de la borrosificación, y combinamos los valores usando el mínimo para el AND, y el máximo para el OR.

R3:	SI	el cliente es	Adulto	AND	el viaje es Corto OR Largo,
		$\mu_{Adulto} = 1.0$		**MIN**	($\mu_{Corto} = 0.0$ **MAX** $\mu_{Largo} = 0.3$)
	$\rightarrow$	la recomendación es	Desaconsejado		
		$\mu_{Desconsejado} = MIN(1.0, MAX(0.0, 0.3)) = 0.3$			







Ejercicio 3: Solución (Conjunto resultado)

- En el método de Mamdani, el conjunto resultado es la unión de los conjuntos resultado de todas las reglas.
- Como los conjuntos "Desaconsejado" y "Recomendado" son simétricos alrededor del 50, cualquier método de deborrosificación nos dará un valor en el que pesará más el que tenga un nivel más alto. El resultado de deborrosificar estará por lo tanto a la derecha del 50, y el viaje se mostrará al cliente.