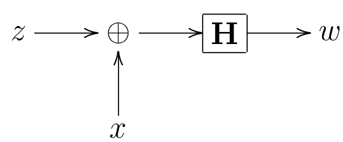
Lógica Computacional 2^o Ano LMCC (2005/06) **Trabalho Prático**

Este projecto é **opcional**. A sua resolução terá um peso de 30% na nota final. O projecto pode ser desenvolvido em grupo (no máximo de 3 pessoas). A apresentação e defesa do projecto decorrerá na semana de 5 de Junho (em dia a anunciar). Na apresentação do projecto deverá ser entregue um pequeno relatório com a descrição da solução apresentada.

Pretende-se que desenvolva, em Prolog, um programa que auxilie a pesquisar a chave de cifragem de uma mensagem. O problema é representado pela figura



e pode ser descrito da seguinte forma: dado um texto de uma mensagem a cifrar z, e conhecendo a SBox $\mathbf{H}$ e o criptograma resultante w, queremos descobrir a chave de cifragem x. Considere que:

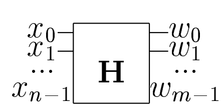
- z e x são sequências de bits do mesmo comprimento n. Ou seja, $z = z_0\, z_1 ... z_{n-1}$ e $x = x_0\, x_1 ... x_{n-1}$.

- $\oplus$ representa o *Xor* bit a bit de duas sequências de bits. O *Xor* é o "ou exclusivo" representado aqui por $+$ e que se define por

$+$	0	1
0	0	1
1	1	0

  Assim, por exemplo, $1010 \oplus 1100 = 0110$.

- $\mathbf{H}$ é uma SBox $n \times m$. Uma SBox é um a "caixa" com n bits de entrada e m bits de saida, em que cada bit de saida w_j depende dos n bits de entrada.



  Assim sendo, $\mathbf{H}$ pode ser vista como um array de m funções n-árias $h_j(x_0, x_1, ..., x_{n-1}) = w_j$, com $j \in \{0, 1, ..., m-1\}$.

O problema proposto reduz-se ao de encontrar as soluções do sistema de equações $\mathbf{H}(z \oplus x) = w$ que, por sua vez é equivalente ao sistema $\mathbf{H}(z \oplus x) + \overline{w} = 1$ (note que a barra representa aqui a negação):

$$\begin{cases} h_0(z_0 + x_0, z_1 + x_1, ..., z_{n_1} + x_{n_1}) + \overline{w_0} & = & 1 \\ h_1(z_0 + x_0, z_1 + x_1, ..., z_{n_1} + x_{n_1}) + \overline{w_1} & = & 1 \\ \qquad\qquad\qquad \cdots & & \\ h_{m-1}(z_0 + x_0, z_1 + x_1, ..., z_{n_1} + x_{n_1}) + \overline{w_{m-1}} & = & 1 \end{cases}$$

Dado que o lado direito de cada uma desta equações é 1, as soluções deste sistema coincidem com as soluções da equação (note que o produto representa aqui a conjunção):

$$\prod_{j \in \{0,1,...,m-1\}} (h_j(z \oplus x) + \overline{w_j}) = 1$$

Portanto, o problema inicialmente proposto reduz-se ao problema de encontrar os modelos que validam a fómula $\prod_{j\in\{0,...,m-1\}}(h_j(z \oplus x) + \overline{w_j})$.

Nos apontamentos teóricos da disciplina encontrará a explicação detalhada de como as fórmulas deste tipo (i.e., polimómios com n variáveis indexadas) podem ser representadas por um *espectro de índices* (i.e. conjunto de conjuntos de inteiros $i \in \mathbb{Z}_n$). Um índice é um subconjunto $u \subseteq \mathbb{Z}_n$.

Uma representação mais conveniente da fórmula para se poder fazer a análise de quais os modelos que a validam, é a sua árvore de fraccionamento. A construção desta árvore pode ser feita usando um método semelhante ao de Davis-Putnam (adaptado agora para lidar com estas fórmulas que apenas têm o "ou exclusivo" e a "conjunção"). A descrição deste método está nos apontamentos teóricos.

Finalmente, a questão de quais os modelos que validam a fórmula

$$\prod_{j \in \{0,1,...,m-1\}} (h_j(z \oplus x) + \overline{w_j})$$

é facilmente respondida por análise da sua árvore de fraccionamento.

Sugestão Divida o problema nas seguintes partes:

1. Definir os predicados que implementam as operações usuais sobre conjuntos.
2. Construir a árvore de fraccionamento de uma função de aridade n, definida por um espectro de índices.
3. Dada uma árvore de fraccionamento de uma fórmula, gerar o conjunto de modelos que validam essa fórmula.
4. Definir perdicados que permitam gerar o conjunto de todos os índices, $\mathbb{U}_n$, e gerar a *união disjunta* e a *convolução* de conjuntos de índices.

5. Definir o predicado que, para uma dada função h_j e uma sequência de bits z (com comprimento igual à aridade de h_j), crie a função $h_j(z \oplus x)$.

6. Definir um predicado que, dada a SBox $\mathbf{H}$, a sequência de bits de entrada z, e a sequência de bits de saida w, construa a fórmula $\prod_{j\in\{0,1,..,m-1\}}(h_j(z \oplus x) + \overline{w_j})$.

7. Defina um programa que receba os dados do problema (i.e., $\mathbf{H}$, z e w) e apresente os possíveis soluções para x (i.e. as possíveis chaves de cifragem).

Explore os aspectos de interface somente depois de ter o problema resolvido.