TP1

> *O propósito deste trabalho é a análise de problemas de alocação usando técnicas de SAT, em lógica proposicional, e IP em lógica linear inteira.*

Exercício 1.1

Pretende-se construir um horário semanal para o plano de reuniões de projeto de uma "StartUp" de acordo com as seguintes condições:

a. Cada reunião ocupa uma sala (enumeradas $1...S$) durante um "slot" $1..T$ (hora, dia).
b. Cada reunião tem associado um projeto (enumerados $1..P$) e um conjunto de participantes. Os diferentes colaboradores são enumerados $1..C$.
c. Cada projeto tem associado um conjunto de colaboradores, dos quais um é o líder. Cada projeto realiza um dado número de reuniões semanais.
d. O líder do projeto participa em todas as reuniões do seu projeto; os restantes colaboradores podem ou não participar consoante a sua disponibilidade, num mínimo ("quorum") de 50% do total de colaboradores do projeto.

São "inputs" do problema:

i. Os parâmetros S , T , P , C
ii. O conjunto de colaboradores de cada projeto, o seu líder e o número mínimo de reuniões semanais.
iii. A disponibilidade de cada participante, incluindo o lider. Essa disponibilidade é um conjunto de "slots" representada numa matriz booleana de acessibilidade com uma linha por cada participante $1..C$ e uma coluna por "slot" $1..T$

São critérios de optimização:

i. Maximizar o número de reuniões efetivamente realizadas
ii. Minimizar o número médio de reuniões por participante.

Exercício 1.2

Na criptografia pós-quântica os *reticulados inteiros* ("*hard lattices*") e os problemas a eles associados são uma componente essencial. Um reticulado inteiro pode ser definido por uma matriz $\mathbf{L} \in \mathbb{Z}^{m \times n}$ (com $m > n$) de inteiros e por um inteiro primo $q \geq 3$.

O chamado *problema do vetor curto* (SVP) consiste no cálculo de um vetor de inteiros

$$e \in \{-1, 0, 1\}^m$$

não nulo que verifique a seguinte relação matricial

$$\forall i < n \,.\quad \sum_{j<m} e_j \times \mathbf{L}_{j,i} \equiv 0 \mod q$$

a. Pretende-se resolver o SVP por programação inteira dentro das seguintes condições
   i. Os valores m, n, q são escolhidos com $n > 30$, $|m| > 1 + |n|$ e $|q| > |m|$.
   ii. Os elementos $\mathbf{L}_{j,i}$ são gerados aleatória e uniformemente no intervalo inteiro $\{-d \cdots d\}$ sendo $d \equiv (q-1)/2$.
b. Pretende-se determinar em, em primeiro lugar, se existe um vetor e não nulo (*pelo menos um dos e_j é diferente de zero*). Se existir e pretende-se calcular o vetor que minimiza o número de componentes não nulas.

Notas

- *Se $x \geq 0$, representa-se por $|x|$ o tamanho de x em bits: o menor ℓ tal que $x < 2^\ell$.*

- *Um inteiro x verifica $x \equiv 0 \mod q$ sse x é um múltiplo de q.*

$$x \equiv 0 \mod q \quad \text{sse} \quad \exists k \in \mathbb{Z} \,.\, x = q \times k.$$

Por isso, escrito de forma matricial, as relações que determinam o vetor $e \neq 0$ são

Por isso, escrito de forma matricial, as relações que determinam o vetor $e \neq 0$ são

$$\begin{cases} \exists\, e \in \{-1,0,1\}^m \;.\; \exists\, k \in \mathbb{Z}^n \quad . \quad e \times \mathbf{L} \;=\; q\,k \\ \qquad\qquad\qquad\qquad\quad \exists\, i < n \quad . \quad e_i \neq 0 \end{cases}$$