Examen Programmation par contraintes IA302

10 novembre 2022

Abstract

Le sujet comporte deux exercices. Le rendu se fera sous forme d'un email (alexandre@ensta.fr) avec en pièce jointe une archive (nom_prenom.zip ou .tar) contenant vos programmes ainsi qu'une copie manuscrite contenant les réponses aux questions (n'oubliez pas d'inscrire votre nom).

1 Problème 1 : Enigma

La machine Enigma est à la source de nombreuses avancées en mathématiques et en informatique. On se propose ici de casser une version simplifiée d'Enigma en utilisant la programmation par contraintes. Enigma, dans une version simple voir Figure 1, se compose de trois rotors et d'un réflecteur. Chaque rotor est une table de transposition (qui change une lettre en une autre) et qui tourne à un rythme particulier. Le premier rotor dit "rapide" tourne d'un cran (donc un décalage dans la table de transposition) à chaque fois qu'une lettre est transposée. Le deuxième dit "moyen" tourne d'un cran lorsque le rapide a fait un tour complet (c'est à dire 26 crans). Enfin le troisième dit "lent" tourne d'un cran lorsque le moyen a fait un tour. Ainsi l'encodage d'une même lettre n'est pas le même à chaque fois, cela rend difficile le cassage du code Enigma. Le réflecteur est également une table de transposition, mais elle est statique et symmétrique. Lorsqu'une lettre est tapée sur le clavier, elle traverse les trois rotors en avant puis elle est transposée par le réflecteur et elle repasse dans les trois rotors au retour. Casser le code Enigma, revient à trouver la position initiale des trois rotors, c'est la clé (trois entiers entre 0 et 25 représentant le décalage des rotors par rapport à la position nulle).

Dans cet exercice, vous allez casser ce code ou plutôt une petite partie, mais le principe est le même.

Pour cela un fichier en Python enigma.py vous est fourni. Il contient les fonctions d'encodage et les paramètres de notre Enigma. Il simule le fait que nous ayons en notre possession une machine Enigma pour essayer de casser le code.

1.1 Question 1 : un seul rotor

Dans un premier temps, les espions adverses n'utilisent que le premier rotor d'Enigma, le"rapide" (sans réflecteur). Nos services secrets ont intercepté un message "BSHCIECWNHN" et également une information importante : on sait que ce message est en anglais et qu'il commence par une formule de politesse comme "HELLO" ou "HI".

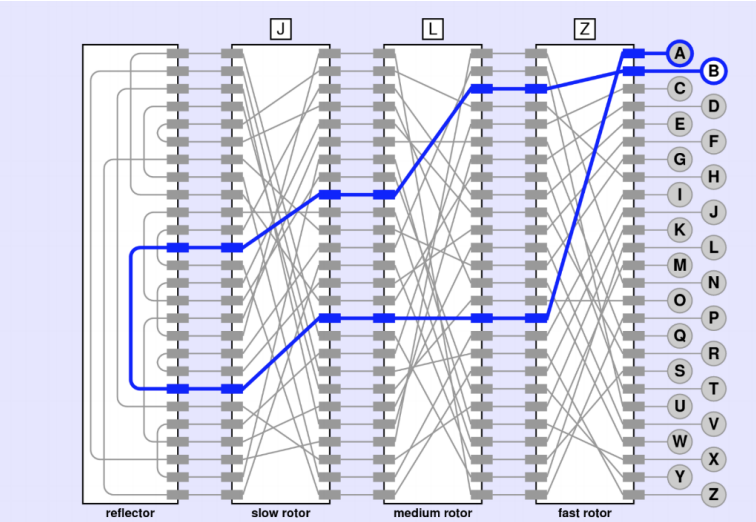


Figure 1: Machine Enigma

1. Ecrivez, dans votre copie, un CSP décrivant le problème consistant à trouver la position initiale du premier rotor (le début de la clé) en fonction des informations obtenues par nos services secrets.

2. Ecrivez un algorithme simple pour résoudre ce CSP dans le fichier fourni et donc trouver la clé.

3. Décryptez le message intercepté avec la clé obtenue et recopiez le dans votre copie.

1.2 Question 2 : deux rotors

Nos ennemis se sont rendu compte que le code était facile à casser avec un seul rotor, ils ajoutent donc un rotor "moyen" (toujours sans réflecteur). Nos services ont intercepté un nouveau message "YELUKSEWOANLGWIFECOHXAHVZ". Ils savent aussi que ce message est en anglais et commence par "THE", "THEY" ou "THIS".

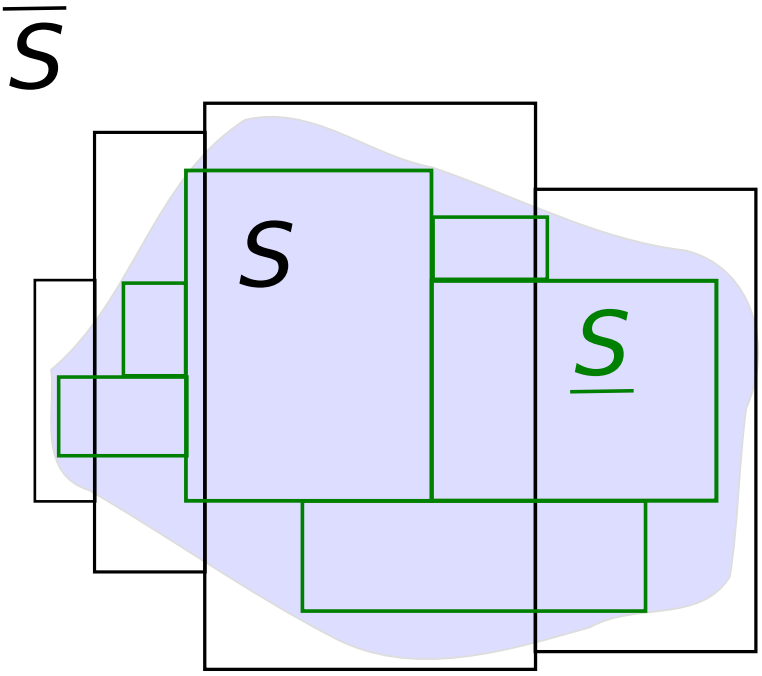
1. Ecrivez, dans votre copie, un CSP décrivant le problème consistant à trouver la position initiale des deux rotors en fonction des informations obtenues par nos services secrets.

2. Ecrivez un algorithme simple pour résoudre ce CSP dans le fichier Python fourni et donc trouver la clé (il peut y avoir plusieurs solutions).

3. Décryptez le message intercepté avec la clé obtenue (trouvez celle parmi les solutions qui décrypte correctement le message) et recopiez le dans votre copie.

2 Problème 2 : le pavage

Soit un ensemble solution à un CSP $\mathcal{S}$, avec un algorithme de branch and prune, nous obtenons un pavage intérieur (tous les points sont solution) $\underline{S}$ et un pavage extérieur (qui contient toutes les solutions) $\overline{S}$ de telle sorte que $\underline{S} \subset \mathcal{S} \subset \overline{S}$. Le dessin ci dessous illustre ce pavage.



2.1 Question 1 : la preuve

Ecrivez, sur votre copie, la preuve qu'un pavage avec un critère d'arrêt de bissection τ plus petit, implique un encadrement de l'ensemble solution plus précis.