Les apports de John Von Neumann et Alan Turing à la modélisation abstraite de ce qu'est un algorithme, Colossus, le cassage d'Enigma et la cryptographie

JULIEN GIRAUD - G2S4
UNIVERSITÉ LYON 1

Alan Turing

Alan Turing est l'un des fondateurs de l'informatique moderne. En 1936 il trouve un moyen de résoudre le problème de l'arrêt. Ce problème consiste à prendre un algorithme en entrée puis à dire en un temps fini s'il va se terminer ou non. Pour résoudre ce problème il invente la « machine de Turing » qui est le concept d'un programme informatique. Il existe donc autant de machines de Turing que de programmes soit une infinité. Il suppose ensuite qu'une machine de Turing permet de déterminer si un algorithme va s'arrêter et il lui transmet un programme qui comporte une boucle infinie. Il faudra donc attendre la fin du traitement de la boucle infinie pour savoir si le programme a une fin. C'est à dire une infinité de temps, ce qui prouve par l'absurde que ce problème est indécidable.
Plus tard il va compléter son concept de machine de Turing avec ce qu'on appelle la « machine de Turing universelle » il s'agit d'une super machine de Turing qui est capable de simuler n'importe quelle machine de Turing avec les mêmes entrées et les mêmes réglages. Il s'agit donc du concept d'un ordinateur moderne.

Durant la guerre il s'est retrouvé à Bletchley Park à travailler au décryptage d'Enigma, la machine qui chiffrait les messages des allemands. Turing a eu une approche particulière pour venir à bout de cette machine, il ne voulait pas juste trouver le code d'un seul message, il voulait mettre en œuvre une machine similaire qui permette de quotidiennement trouver le réglage d'Enigma. Son idée reposait à la fois sur une machine de Turing capable de tester un très grand nombre de réglages mais aussi de prendre en compte les erreurs humaines pour réduire les possibilités (redondance dans les messages comme « Heil Hitler » ou habitude d'écriture des chiffreurs). La machine qu'il a conçu porte de nom de « bombe de Turing ». Il s'agit alors d'une des machines des plus complexe jamais créée. Cette machine et le travail acharné de Turing au décryptage des messages allemands auraient permis de terminer la guerre environ deux ans plus tôt. Le secret a ensuite été gardé jusque dans les années 70 où certains ont recommencé à parler de cette machine. Officiellement ce n'est qu'en 2000 que la Grande Bretagne a publié ces travaux secrets.

Turing a également travaillé à la création des premiers ordinateurs, d'abord sur le projet ACE (Automatic Computing Engine). Il a complété les travaux de John Von Neumann en utilisant son système de structure d'ordinateur et en détaillant son fonctionnement surtout du point de vue programmation. Cependant le projet n'a pas abouti, en partie à cause de son côté solitaire toujours associé aux informaticiens. Comme quoi certaines choses ne changent pas. Finalement il a dirigé le développement de l'un des premiers ordinateurs industrialisés : le « Manchester Mark I ».

Colossus

Colossus est le nom d'une série de calculateurs électroniques. L'objectif de ces machines était de décrypter le code des téléscripteurs de FISH, un autre système de chiffrement allemand qui servait à chiffrer les communications vocales des haut dirigeants. La première machine de cette série est le premier grand calculateur électronique de l'histoire, crée à Dollis Hill en 1943. Le nom de Turing est souvent associé à ces machines, il n'a pourtant aucun rapport avec leur conception mais il les a vu à l'œuvre.

John Von Neumann

Neumann a beaucoup apporté à l'informatique moderne. Il est notamment à l'origine de l'architecture des composants de l'unité centrale d'un ordinateur, toujours utilisé de nos jours dans la plupart des ordinateurs. Inspiré par le travail de Turing et son concept de machine de Turing, il cherche à concrétiser la conception d'une telle machine. Le système qu'il propose permet de modéliser une machine de Turing universelle. Ce système possède une entrée et une sortie tous deux reliés à une unité de traitement. Cette unité de traitement effectue les opérations de base, elle est reliée à une unité de contrôle qui lui indique l'ordre dans lequel effectuer les opérations. Enfin les deux unités sont reliées à une mémoire qui contient à la fois le code à exécuter et les données passées en entrée. Au final il attribue son modèle de « calculateur à programme » à Turing qui concrétisera ce projet.

Sources :

https://fr.wikipedia.org/wiki/Alan_Turing
http://www.cite-sciences.fr/fr/au-programme/lieux-ressources/bibliotheque/chercher-trouver/sinspirer/dossiers/alan-turing/
https://www.la-croix.com/Culture/TV-Radio/Ce-lon-doit-Alan-Turing-2018-08-13-1200961465
https://dossiers.lalibre.be/turing/
https://lejournal.cnrs.fr/articles/alan-turing-genie-au-destin-brise
Le film « Imitation Game » de 2014
https://fr.wikipedia.org/wiki/Colossus_(ordinateur)
https://fr.wikipedia.org/wiki/John_von_Neumann
https://www.techno-science.net/definition/6495.html
http://www.universalis-edu.com/encyclopedie/john-von-neumann/