



Turing, le père oublié de l'informatique

CYBER HÉROS • Alan Turing fêterait demain son centième anniversaire. Auteur de l'article fondateur de la science informatique, ce Britannique excentrique, mort en 1954, avait aussi contribué au décryptage d'Enigma.

PROPOS RECUEILLIS PAR PASCAL FLEURY

«Chaque ordinateur est une incarnation d'une machine de Turing.» La formule du «Time Magazine» en dit long sur ce Britannique peu connu du grand public, et pourtant considéré comme le père de l'informatique. Professeur émérite en informatique à l'Université de Fribourg, Jürg Kohlas lui rend hommage, alors que s'ouvre aujourd'hui à Manchester une conférence marquant le centième anniversaire de la naissance de ce «Newton de l'informatique», et que de nombreux autres événements sont programmés en son souvenir de par le monde. Rencontre.

Alan Turing est reconnu comme le père de l'informatique. Comment se fait-il qu'il soit si peu connu du grand public?

Jürg Kohlas: En fait, Alan Turing est assez célèbre en Angleterre et aux Etats-Unis. Il a été classé parmi les cent personnalités les plus importantes du XX^e siècle par le magazine «Time». Turing est le père de la partie théorique de l'informatique. Lui-même n'a pas construit d'ordinateur, mais seulement élaboré un modèle conceptuel. Si les constructeurs d'ordinateurs, comme Bill Gates ou Steve Jobs, sont devenus plus populaires, c'est que l'informatique n'est souvent connue que par ses applications, et non par ses théories. C'est là un défaut de notre système de formation. Turing est à l'informatique ce que Newton est à la physique. D'autres chercheurs, comme Church, Post ou Markov, ont développé des modèles de calculs équivalents, mais le modèle de Turing reste le plus simple.

Quelle théorie a-t-il établi?

Il a défini formellement ce que veut dire «calculer automatiquement». C'était en 1936 à l'Université de Cambridge, alors qu'il a 24 ans. Pour y parvenir, il a étudié rigoureusement le processus mental des «computers», ces comptables qui, à l'époque, passaient leurs journées à faire des calculs à la main, dans des banques ou des assurances. Il a isolé chaque état de leur réflexion durant leurs calculs, puis a formalisé leur pensée en un modèle conceptuel qu'on a appelé la «machine de Turing». C'est un modèle universel. Tout ce qu'on peut calculer avec un ordinateur moderne, et tout ce qu'on pourrait calculer à l'avenir, peut être calculé par la «machine» abstraite de Turing.

Quelle est l'importance de sa découverte?

Le modèle permet de déterminer ce qui peut être calculé et ce qui ne peut pas l'être. Toutes les applications informatiques, dans tous les domaines de la société, se basent sur cette notion de calculabilité. Il faut savoir que les ordinateurs ont de réelles limites. Certains problèmes, pourtant facile à énoncer, ne peuvent pas être résolus par l'informatique. C'est ce qui se passe avec les para-



Sculpture à la mémoire d'Alan Turing, dans un parc de Manchester. Le mathématicien tient une pomme à la main, en référence à son tragique empoisonnement au cyanure, à l'âge de 42 ans. DR

doxes. On connaît bien le paradoxe classique du Crétois qui dit: «Tous les Crétois sont des menteurs.» Idem en mathématiques: si l'énoncé est «ce théorème n'est pas démontrable», le théorème est vrai, mais pas démontrable. Parce que s'il était démontrable, alors il serait faux.



«Turing est à l'informatique ce que Newton est à la physique»

JÜRIG KOHLAS

La «machine de Turing» est aussi un outil pour estimer la difficulté des problèmes informatiques...

Elle est utilisée pour mesurer la complexité des problèmes à résoudre, pour savoir si l'on peut en venir à bout dans un temps et avec des ressources de mémoire raisonnables. Si, par exemple, un conseiller fédéral désire faire le tour des villages suisses, il devra attendre des milliards d'années pour qu'un ordinateur lui trouve exactement le chemin le plus court. Grâce à la «machine de Turing», on peut cerner les problèmes et estimer leur complexité. C'est comme en physique. On pourrait construire un pont sans connaître les lois de Newton.

Mais si l'on veut qu'il tienne, on a meilleur temps de les appliquer!

Le modèle de Turing permet aussi de déterminer ce qui est aléatoire. Quelle importance cela a-t-il?

C'est très utile dans les domaines de la cryptographie, de la sécurité ou encore des jeux. Dans ces domaines, il est important de garantir des séquences de chiffres les plus aléatoires possibles afin d'éviter tout piratage ou tricherie. Or, pour déterminer si un programme est vraiment aléatoire, les théories de probabilités et de statistiques ne suffisent pas. Le modèle de Turing permet en revanche d'être au clair.

Les travaux fondamentaux de Turing ont-ils directement influencé la construction des ordinateurs?

Turing a eu surtout une influence dans le développement de la recherche fondamentale. Mais après avoir publié son travail, il a aussi rencontré le mathématicien américano-hongrois John von Neumann à Princeton, considéré comme le père de l'architecture de tous les ordinateurs. On pense que Turing l'a influencé avec sa «machine» universelle, qui peut simuler toutes les autres

machines. Or, c'est cela l'idée de l'ordinateur de Neumann: une machine mathématique, qui n'est rien en soi, mais qui commence à fonctionner lorsqu'on lui donne un programme et des données. Cette idée de la machine universelle, capable de résoudre tous les problèmes de traitement d'informations, remonte bien à Turing. Les premiers constructeurs n'ont cependant pas vu que leurs machines pouvaient avoir un usage vraiment universel, non seulement dans les laboratoires, mais dans les bureaux et les ménages.

Turing a-t-il travaillé lui-même sur des prototypes d'ordinateurs?

Il a participé à la conception du premier ordinateur numérique Colossus, qui a servi à décoder les messages allemands de haute importance pendant la Seconde Guerre mondiale (lire ci-dessous). Après 1945, il a aussi travaillé à la conception de l'ordinateur ACE (Automatic Computing Engine) au Laboratoire national de physique, à Teddington, puis à la programmation d'un des tout premiers véritables ordinateurs: le Manchester Mark I, en 1948, à l'Université de Manchester.

Alan Turing s'est-il déjà intéressé à l'intelligence artificielle?

LA POMME EMPOISONNÉE

Alan Turing est né le 23 juin 1912. Génie remarqué par ses maîtres à 6 ans, assidu au point de parcourir 90 km à vélo pour se rendre en classe alors que les trains sont en grève (il était aussi bon marathonnien), familier des travaux d'Einstein dès l'âge de 16 ans, il publie son article fondateur de la science informatique en 1936, au King's College à Cambridge. Pendant la guerre, son engagement auprès des services secrets (lire ci-dessous) lui impose une pause académique, mais ne l'empêche pas de poursuivre ses recherches. On le retrouve dès 1945 au National Physical Laboratory à Teddington, puis à la direction du tout nouveau laboratoire d'informatique de l'Université de Manchester.

Sa carrière est soudainement brisée en 1952. Alors qu'il vient d'être consacré membre de la Royal Society, il est condamné pour homosexualité à la castration chimique. Écarté des grands projets scientifiques, il se donne la mort par empoisonnement au cyanure le 7 juin 1954, vraisemblablement en croquant une pomme, comme dans le film «Blanche-Neige», qu'il adorait. On a vu parfois dans l'emblème d'Apple un hommage au père de l'informatique. Mais le premier logo d'Apple représentait Newton sous son pommier... PFY

Il est l'un des premiers à y avoir pensé. Il s'est très vite demandé si les ordinateurs pouvaient jouer aux échecs. Il s'est intéressé à mesurer l'intelligence des machines. Il a mis au point le «test de Turing» dans ce but. Le principe consiste à poser des questions à l'ordinateur. Si les réponses laissent subsister un doute sur une origine humaine, l'ordinateur est considéré comme intelligent. Le programme informatique ELIZA, écrit par Joseph Weizenbaum en 1966, et qui simulait les réponses d'un psychothérapeute, allait dans ce sens. Il aurait presque pu passer le test de Turing.

A la fin de sa vie, Alan Turing s'est aussi intéressé à la biologie...

Il a élaboré un modèle biomathématique pour la morphogenèse (structure des organismes vivants), et a écrit un article assez fondamental sur le sujet. C'est bien ce qui caractérise son génie: il s'est sans cesse attaqué à de nouveaux problèmes, cherchant constamment de nouvelles solutions. Même lorsque la chaîne de son vélo s'est mise à dérailler! Observant que l'incident se produisait tous les 14 tours de roue, il a préféré installer un compteur de tours pour prévenir la panne plutôt que de réparer le pignon! C'est assez typique d'un mathématicien...!



Réplique de la «bombe de Turing» au Musée de Bletchley Park. DR

Une «bombe» contre Enigma

Durant la Seconde Guerre mondiale, Alan Turing a mis toute sa science au service des forces alliées. Engagé au quartier général des Services du chiffre britannique, dans le manoir de Bletchley Park, il a été l'un des principaux contributeurs aux recherches qui ont permis de «casser» les codes secrets des machines d'encryptage nazies Enigma et Lorenz.

Génie insoupçonnable, sous ses allures excentriques, – il roulait parfois à vélo avec un masque à gaz pour se prémunir du rhume des foies! –, il n'en était pas moins «Le Prof» de Bletchley Park, comme le surnommaient les cryptologues, mathématiciens, traducteurs, linguistes, joueurs d'échecs et autres cruciverbistes qui formaient l'étonnante équipe de recherche

secrète de l'opération «Ultra». Bénéficiant des travaux réalisés sur Enigma par les services secrets polonais, et en particulier par le mathématicien Marian Rejewski, Turing commence par mettre au point dès 1940, avec William Gordon Welchman, une «bombe» cryptologique plus rapide et plus efficace que celle des Polonais. Cette machine livrait les clés de décodage des messages nazis, quelle que soit la complexité de leur encryptage.

En 1942, Turing se rend aussi aux Etats-Unis pour tenter de casser des codes japonais. Il y rencontre Claude Shannon, l'inventeur de la théorie de l'information, qui a popularisé l'utilisation du mot «bit» comme mesure élémentaire de l'information numérique. De retour en Angleterre,

il travaille au décodage des messages générés par la machine de Lorenz, utilisée pour les communications ultrasecrètes entre le Führer et les quartiers généraux des armées. Ses résultats sont aussitôt exploités par le mathématicien Max Newman, qui conçoit le Colossus, premier ordinateur électronique basé sur le système binaire, opérationnel dès la fin 1943.

En 1945, le héros de l'espionnage est récompensé de l'Ordre de l'Empire britannique. Mais son rôle primordial dans le décryptage des codes nazis, qui a contribué à la victoire des Alliés, est tenu secret jusqu'aux années 1970. Alan Turing, décédé tragiquement en 1954, n'en a jamais récolté les lauriers. PFY

SEMAINE PROCHAINE

LES POUBELLES RADIOACTIVES

Où finissent les déchets radioactifs des centrales nucléaires? Un dossier réalisé dans une France qui s'accroche encore à l'atome. Pour sa part, RTS-La Première diffuse dès lundi son dernier volet sur le processus de Bologne. Ce dimanche, pas de documentaire TV «Histoire vivante» en raison de l'Euro 2012.