Donner du sens aux éléments de technologie : jouons avec nos enfants

Pour citer cet article :

Alvarez Aurélien, Garreau Pascal, Tort Françoise et Viéville Thierry (2014). Donner du sens aux éléments de technologie : jouons avec nos enfants. Premier volet d'une série de deux articles *Adjectif.net*, [En ligne] http://www.adjectif.net/spip/spip.php?article288

Résumé :

Le BO°8, 13/11/2011 de l'enseignement de spécialité Informatique et Sciences du Numérique (ISN) précise la finalité de cet enseignement « maîtriser les mécanismes fondamentaux qui régissent ces mutations [du numérique] et être en mesure d'apprécier les enjeux sociétaux qui en découlent ». Un élément clé est de *donner du sens aux éléments de technologie et à leurs usages*. Notre thèse va être ici de montrer qu'apprendre à « coder » (d'aucuns diront programmer) n'est qu'un marchepied pour apprendre à *décoder* le numérique, du plus petit à la plus grande d'entre nous.

Mots clés :

Apprentissage de l'informatique, enseignement de spécialité Informatique et Sciences du Numérique (ISN)

par A. Alvarez, P. Garreau, F. Tort et T. Viéville

Si nous n'avons pas de recul suffisant (en tout cas en France), pour théoriser cela, nous avons déjà beaucoup d'exemples de réussites concrètes. Nous allons donc très simplement en partager quelques-unes et soumettre au lecteur les leçons que nous pensons en avoir tiré. Voici donc un témoignage commenté d'actions de médiation scientifique sur le terrain.

Voir l'activité complète et la vidéo pour les enfants : "Dis maman (ou papa), c'est quoi un algorithme dans ce monde numérique ?"

Nous voilà en famille. Elle ou il s'ennuie du haut de ses 5 à 7 ans, il faut trouver un jeu rigolo. Par exemple, le jeu du « robot-idiot » qui doit sortir d'un petit labyrinthe que l'on aura construit dans le séjour en déplaçant quelques tables ou chaises, ou en le dessinant à la craie sur le sol de la cour. Celui qui joue le rôle du robot n'a pas le droit de comprendre le langage humain, mais juste un langage très limité : « avancer », avancer d'un pas ; « gauche », tourner à gauche d'un quart de tour ; « droite », tourner à droite d'un quart de tour. On lui donnera une séquence de ces cartes-instructions qui sera son « algorithme » à exécuter sans réfléchir.

Le jeu pourra se compliquer s'il y a une porte (concrétisée par un objet quelconque) qui peut être fermée ou ouverte, sans qu'on le sache à l'avance. Il faudra alors introduire une condition dans notre algorithme : « si la porte est fermée alors [fais le tour] »… et d'expliquer en détail ce que veut dire « fais le tour » ! Pour robot-idiot, il y aura alors deux paquets de cartes à choisir selon la condition.

Ensuite on aura sûrement envie de ne pas répéter « avance d'un pas, avance d'un pas, avance d'un pas » mais « avance de trois pas ». Donc l'instruction aura une valeur variable qui permettra d'avancer plus efficacement. Avec un crayon à papier et une gomme, on pourra mémoriser la valeur et l'effacer ensuite sur la carte.

On pourra vouloir encore utiliser une boucle « tant que tu n'es pas sorti du labyrinthe, avance tout droit jusqu'au prochain carrefour puis prends à droite » : est-ce que ça marche pour tous les labyrinthes ? C'est une question à tester expérimentalement…

Ce jeu du « robot-idiot » n'est pas du tout original, il correspond à une activité débranchée que l'on appelle la « tortue-logo » ; il semble que ce soit la façon la plus répandue d'apprendre les ingrédients des algorithmes aux enfants, ici sous sa forme minimale.

Le point clé, c'est que l'enfant apprend à travers des gestes sensorimoteurs, car c'est ainsi que dans notre cerveau les concepts les plus abstraits se forment. C'est donc à travers les mises en situation les plus simples que se forme son bel et jeune esprit, contrairement aux robots et aux ordinateurs qui, eux, restent de parfaits imbéciles.

Que venons-nous d'apprendre ici ?

Quelque chose de parfaitement inutile, mais totalement indispensable à l'éducation au numérique.

Tout d'abord que pour exprimer un algorithme il y a quatre ingrédients : une séquence d'instruction, des variables, des tests et des boucles. Avec ces ingrédients, nous pouvons (faire) exécuter *tous les algorithmes* du monde. Car tout ce qui se passe dans un smartphone, une tablette, une télévision numérique, un robot ou un ordinateur se réduit à ces ingrédients (en quantité géante).

Cela signifie que nous avons caractérisé ce qu'est l'intelligence mécanique. Sauf bouleversement de la science, aucun système artificiel, aucun robot ne saura faire autre chose qu'exécuter ces algorithmes. Les ordinateurs ne font pas plus que ça. De manière fabuleusement rapide et avec des algorithmes fabuleusement plus longs, certes. Mais pas plus.

Cerveau, ordinateur ? Deux profs de philo aident à se libérer de l'amalgamme.

Cette initiation sera le point de départ pour montrer tranquillement à l'enfant que plein de choses qu'il fait avec son cerveau (compter, trier des objets, rechercher un mot dans un texte, etc.) peuvent être faites par une machine, car cela se réduit à un algorithme. Mais que faire un dessin qui soit joli, choisir sa ou son meilleur-e ami-e, inventer une danse, appartiennent à une autre forme d'intelligence, très différente. L'enfant a donc appris en jouant un premier rudiment de pensée algorithmique.

Mais il y a encore plus important : nous sommes en train de l'aider à dé-personnifier *l'ordinateur*. De la légende de Pinocchio au mythe du Golem, nous autres humains (surtout les garçons) avons ce fantasme récurrent de créer un être animé, vivant, sans passer par le paradigme biologique usuel (dans *Le Livre du ça*, 1923, Georg Grodeck décrit bien ce mythe humain récurrent). Or, si nous voulons que ne se confondent pas science et science-fiction, que soient dépassés les articles de science-spectacle qui montent en épingle un résultat scientifique pour conclure par un « pourquoi pas ? » en jouant justement sur les mythes que nous véhiculons, alors commençons par montrer qu'il n'y a rien de magique dans les ordinateurs. Il n'y a que des algorithmes. Qui calculent fabuleusement vite mais sont totalement dénués de pensée.

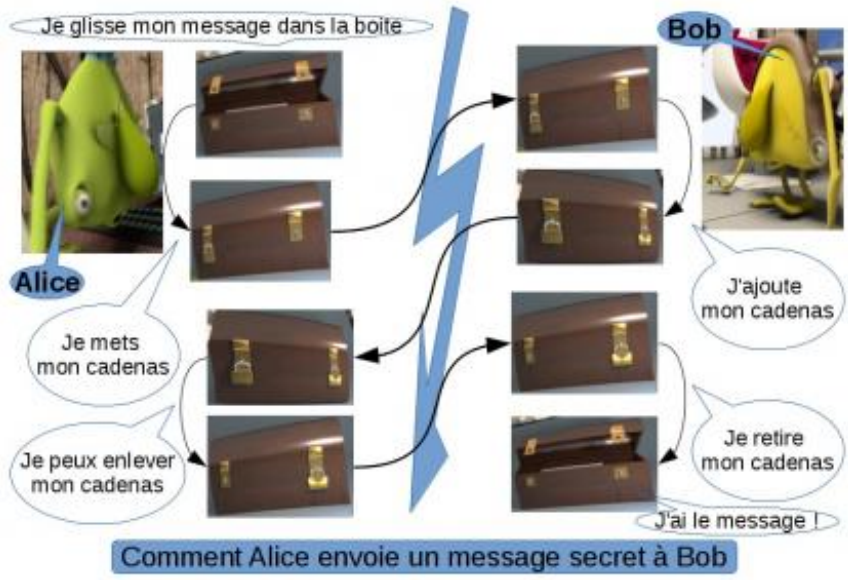
Nous sommes donc bien dans un apprentissage de savoir, savoir-faire et savoir-être.

Ceci étant : peut-on et faut-il apprendre à coder des algorithmes à toutes et tous dès le plus jeune âge ? Il nous semble que oui. Sûrement pas pour devenir informaticien. Disons plutôt pour survivre à l'informatique.

Voir l'activité complète et la vidéo pour les enfants : "Dis papa (ou maman), comment on cache des secrets dans le monde numérique ?"

Elle ou il a grandi. Disons d'une dizaine d'années. Lui permettre de vivre Internet sans crainte, donc de comprendre, entre autres, comment fonctionnent cryptage et authentification, devient une nécessité. Or, échanger des informations qui restent secrètes sur Internet pose un problème très particulier : il faut que deux personnes, qui ne se connaissent peut-être pas, qui ne peuvent communiquer que publiquement devant tout le monde (Internet est un espace public) donc sans s'envoyer aucune information privée, puissent tout de même s'envoyer un message secret qu'elles seules pourront lire, en étant sûres que personne n'ait volé leur identité.

Une telle solution existe. C'est le cryptage à double clé. Il est très important de comprendre comment cela marche, sinon ces mécanismes resteront mystérieux, magiques, au lieu de pouvoir être vus comme des actes du quotidien. La bonne nouvelle est que c'est facile à expliquer. Voici, sous forme graphique, comment jouer avec un objet concret pour faire comprendre ce mécanisme.



Comment Alice envoie un message secret à Bob

Bien entendu, dans le monde numérique, ce qui tient lieu de « cadenas », c'est un calcul qui va prendre le *message initial* et le mélanger avec une formule mathématique pour en faire un *message crypté*. De ce calcul, seul l'émetteur du message a la clé (c'est-à-dire le code pour réaliser le calcul à l'envers afin de retrouver le message initial). Ici on voit que chacun applique son calcul de mélange, puis de démêlage. On note aussi que, pour que ça marche, il faut pouvoir intervertir les deux calculs puisque le démêlage par l'émetteur se fait sur le message mélangé par le récepteur.

On note aussi qu'il faut que les personnes soient bien identifiées, car si un personnage malicieux se fait passer pour Bob au début de l'échange, alors il volera le message d'Alice, de manière tout à fait sécurisée !

Nous allons donc aussi jouer à ce jeu « à l'envers » pour non plus crypter un message mais authentifier une personne de manière sûre. Un des joueurs sera « l'autorité » une personne en qui nous avons, toutes et tous, toute confiance. Chaque joueur a un cadenas qu'il va remettre à l'autorité. Celle-ci va bien noter à qui ils appartiennent. Ensuite les joueurs vont se cacher sous un masque. Quand, disons Alice, voudra savoir qui est vraiment Bob, alors elle va demander à l'autorité un cadenas qui appartient à Bob, elle va mettre un code dans une boîte, qu'elle va fermer par ce cadenas. Seul le vrai Bob, celui qui a la clé, pourra ouvrir le cadenas, donc prouver son identité : *s'authentifier*. On rendra explicite que le cadenas est une « clé publique » tandis que la combinaison du cadenas (ou la clé du cadenas) est la « clé privée ». La mise en œuvre du jeu est discutée dans

l’article cité dans le QR-code.

Que venons-nous d’apprendre ici ?

Faire comprendre le principe du cryptage à clé publique ou cryptage asymétrique permet de susciter la réflexion sur plusieurs choses.

D’abord, le fait qu’un algorithme peut servir à quelque chose de précieux comme protéger ses secrets et que cet algorithme ne s’applique pas que sur des calculs numériques mais aussi à toutes sortes de données. On vient donc de montrer que le fait que des données (textes, sons, images, ..) soient devenues numériques permet de traiter l’information qu’elles contiennent avec des fonctions « universelles » : mémoriser, transmettre, dupliquer, compresser, crypter nos données se font avec des mécanismes similaires, quelle que soit leur nature. C’est un bouleversement par rapport au temps où la musique était sur des disques vinyles et les photos sur des plaques argentiques.

Plus prosaïquement, le fait de « comprendre comment ça marche » permet de ne pas se « faire avoir par les autres ». À l’inverse, utiliser un mécanisme sans bien le comprendre, nous rend bien vulnérables. On entre ainsi dans le domaine de la maîtrise des usages du numérique, qui inclut la question de la sécurisation de nos données et de notre identité.

On découvre aussi comment marche l’authentification, cette procédure qui consiste à vérifier l’identité d’une entité (personne ou mécanisme numérique). Elle utilise à la fois (i) une opération que seule la personne peut effectuer [1] et (ii) une autorité de certification (organisme indépendant) auprès de laquelle on dépose la clé publique [2] et qui va vérifier par des moyens solides que le déposant n’usurpe pas une identité.

On peut profiter de cette activité pour expliquer que dès qu’un algorithme sera assez puissant pour énumérer toutes les combinaisons du cadenas (toutes les clés privées) alors le code sera cassé. Ou que si un pouvoir militaire ou politique viole la confiance accordée à l’autorité de certification, alors l’édifice s’écroule. Paradoxalement peut-être, on constate que faire comprendre comment ça marche et montrer les limites de cette sécurité informatique, rend les gens non pas plus méfiants, mais plus lucides. Ce qui a changé, c’est que le danger n’est plus du domaine de l’inexpliqué, mais que citoyennes et citoyens sont éclairés sur le sujet.

Un jeu sérieux « l’isoloir » permet aux plus grands de faire l’expérience de l’action citoyenne éclairée de savoirs divers, y compris informatiques.

En faisant cette activité, une autre « découverte » s’impose (sic) : les maths servent à quelque chose ! Inutile de scander ou de tenter de décréter que sciences informatique et mathématiques servent à quelque chose : prouvons-le par l’exemple. Celui-ci en est un joli. Pas besoin de beaucoup de mathématiques pour commencer (si on décide d’être dans un monde où la « division » n’existe pas, alors multiplier des chiffres permet de crypter un message !), mais on peut aussi aller loin en arithmétique ou en algèbre pour les "mathophiles".

Cette activité est un exemple de ce qu’il faut apprendre, pour aborder les grandes problématiques sociétales de l’informatique. Ce qu’est la neutralité du net avant de parler de liberté d’expression numérique, ce qu’est un bien non rival avant de parler de droit d’auteur numérique, ce qu’est l’hypermnésie des données numériques avant de parler de vie privée en sont les autres exemples les plus importants. Cela reste assez facile (ne croyez pas ceux qui ont sur-compliqué ces savoirs, par pédantisme ou absence de connaissances techniques).

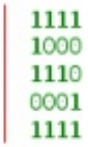
Bref : est-il utile d’apprendre les usages du numérique à partir de la découverte de l’informatique ? Il nous semble que oui, que c’est facile et que cela change notre façon d’être face au numérique.

Voir l'activité complète et la vidéo pour les enfants : "Dis maman (ou papa), mais comment sont codés les objets numériques ?"

Plus facile à décliner, il y a un autre volet important de l'apprentissage des fondements du numérique, c'est la façon dont sont codés les objets.

Ce qui est remarquable c'est que tous les nombres, les textes, les sons, les images, les informations ont un reflet numérique, un codage. Avec un bit, on va par exemple coder une réponse « oui » ou « non », disons 0 ou 1. Avec deux bits qui prennent chacun la valeur 0 ou 1, on dispose de quatre codes 00, 01, 10, 11 et on peut coder ainsi quatre éléments, quatre couleurs ou quatre lettres, ou les nombres de 0 à 3 inclus. Avec plus de bits on codera des nombres plus grands, toutes les lettres, etc.

On pourra, pour illustrer très simplement ce point, proposer, par exemple, un langage pour coder un tout petit dessin. Au niveau binaire, il faut coder chaque pixel. L'idée est que c'est amusant de donner un code 11111000111000011111 qui, une fois « décodé en 2D », donne un digit, ici une sorte de « S ». Deux enfants ou groupes d'enfants se mettent de part et d'autre d'un paravent. On convient qu'ils vont s'échanger de tous petits dessins sur une grille de taille 4 x 5 par exemple. On y dessine des points (disons un 1) ou pas de point (disons un 0) et cela fait des chiffres ou des lettres. Ensuite on transmet à la queue leu leu les bits et l'autre groupe dessine le résultat et le dessin ré-apparait.



Si par exemple on oublie de transmettre un des bits ça ne fait pas juste une erreur, c'est toute l'image qui se décale et ça donne n'importe quoi. On pourra même s'amuser à envoyer les bits en verlan, du dernier au premier, et voir ce qui se passe pour le dessin.

Qu'apprenons-nous avec eux ici ?

Tout d'abord, on concrétise ici cette idée, souvent bien vague, que « les objets sont codés en binaire dans les ordinateurs ». On voit d'abord que ce codage est un choix, une convention entre les individus, exactement comme le langage. On expérimente qu'il est possible de coder toutes sortes d'objets, en fait tous les objets que nous trouvons sur Internet ou dans nos smartphones.

Ce qui est intéressant pour l'enfant, c'est que cela va l'aider à faire la différence entre le réel et le virtuel. Le codage d'un son ou d'une scène visuelle n'est que le reflet numérique de cet objet réel. Il y a le « S » que je dessine avec de la peinture, il est fait de matière. Il y a ensuite le codage du « S », ce paquet de 0 et de 1, qui ne représente le « S » que parce qu'on le veut bien.

C'est important d'aller assez loin avec cette métaphore et de montrer que, par rapport à une rencontre réelle entre deux amis, la communication à travers un réseau social n'est qu'un échange de codes informatiques. On ne peut pas être bien ensemble sur un réseau social, on ne peut que se le figurer. Une personne que nous ne connaissons que par son profil d'un réseau social n'existe finalement qu'à travers les informations qui sont partagées. Le « reste », c'est nous qui l'avons imaginé. Ce peut-être une expérience très intéressante, en soi, où chacun se sent effectivement bien de son côté mais qui ne met en jeu qu'une partie de deux êtres qui communiquent ainsi. Cette expérience est donc, par définition, d'une tout autre nature qu'une véritable rencontre réelle entre deux amis qui peuvent véritablement éprouver, expérimenter le fait d'être « bien ensemble ».

À un niveau plus technique, on va aussi rapidement réaliser que l'information, par ce mécanisme de codage informatique, devient une matière abstraite qui se mesure.

Conclusion : "dis mon enfant, que vas-tu faire de ce monde numérique qui est tien ?"

Initiés aux fondements des algorithmes, rassurez-vous cependant, tous les enfants ne deviendront pas (forcément) geeks ou matheux ! Tels que nous concevons ces apprentissages, ils ne devraient ni ôter la magie du monde aux poètes en herbe, ni forger une armée d'informaticiens. Juste donner à toutes et à tous les clés de la citoyenneté à l'ère de la société de l'information et leur permettre d'être acteurs de son devenir – s'ils le souhaitent bien sûr ! Ce qui n'est, après tout, pas si mal.

Références :

- education.gouv.fr (2011) programmes des classes terminales des voies générale et technologique *BO°8, 13/11/2011*
- tralalere.com et al (2011) Internet sans crainte *http://www.internetsanscrainte.fr*
- Aurélien Alvarez, et al (2014) Dis maman (ou papa) … trois articles sur les algorithmes, le codage et la cryptographie *http://images.math.cnrs.fr*
- Aurélien Liarte, Yves Geffroy (2008) Le cerveau, un ordinateur ? *https://interstices.info*
- tralalere.com, inria.fr et al (2013) L'isoloir Faites l'expérience de l'action citoyenne, votez avec votre tête *http://www.isoloir.net*

[1] Message sur son téléphone portable - supposant qu'il est bien en sa possession -, mot de passe, ici un calcul qui a besoin d'une clé publique (que tout le monde connaît) et une clé privée (qu'il est le seul à détenir et n'aura jamais communiqué à personne).

[2] Cette opération lourde se fait une seule fois et reste valide tant que la clé privée n'est pas ventilée. Ensuite c'est auprès de cette autorité que l'on récupère la clé publique pour demander de manière sûre à une personne le calcul d'authentification avec une clé privée.