Codage, codes, signes,

de la sémiotique aux mathématiques

Signes, sémiotique

La sémiotique (ou sémiologie) est la science qui étudie les signes et leurs significations ; le signe pouvant être défini comme un « *objet matériel, perceptible, valant pour une chose autre que lui-même qu'il évoque ou représente à titre de substitut* » (TLFi).
D'un point de vue sémiotique, un code est un système de symboles permettant de représenter une information ou un objet. Le signe renferme à la fois le symbole utilisé (le signifiant) et l'information ou l'objet auquel ce symbole renvoie (le signifié).
Ainsi, en mathématiques, l'écriture des chiffres (1, 2, 3, 4, 5, 6, 7, 8, 9, 0), par exemple, est un système de signes permettant l'écriture des nombres en lien avec une théorie (l'écriture décimale de position en base dix). Il n'y a pas en particulier de lien entre le code et une représentation imagée de l'objet représenté ; même si le signe utilisé pour le chiffre 'un' peut être schématiquement associé à l'unité (I, |, 1. . .), 2, 3, ou les autres chiffres ne sont pas des représentations schématiques du signifié.
Pour aller plus loin.

D'un point de vue didactique, les différentes représentations d'un même objet construisent le sens de cet objet. Ainsi, dans les séquences présentées, le lien entre l'objet (le son) et le code passe par une mise en relation de l'un à l'autre et donc par la correspondance bijective entre deux ensembles. Le travail sur le codage peut donc être lié à la découverte de cette correspondance inversible.
Pour aller plus loin.

En prolongeant un peu l'usage des codes, la cryptographie est la science permettant de modifier un codage en un autre de façon suffisamment simple pour qu'il soit possible relativement facilement de passer d'un code universellement connu à cet autre système de codage, pour que la traduction inverse soit difficile sans une clef et facile avec. Il y a donc dans l'idée de codage, l'idée sous-jacente de correspondance bijective (un à un) et de d'inversibilité.
Pour aller plus loin.

Gilles Aldon, IFÉ-ENS de Lyon
Lyon (EducTice-S2HEP, Centre Alain Savary)–DSDEN de Côte d'Or–Ville de Dijon
http://ife.ens-lyon.fr/sciences21

Ferdinand de Saussure (1857-1913), linguiste Suisse et Peirce (Charles Sanders Peirce, 1839-1914), philosophe et scientifique américain sont considérés comme les deux pères de la sémiologie. Leurs approches sont complémentaires, linguistique et logique ; ces deux champs s'intéressent aux signes et ont conduit Saussure et Peirce à les caractériser par leur composante matérielle, le signifiant (le representamen pour Peirce) et leur partie abstraite et conceptuelle, le signifié.

Nous appelons signe la combinaison du concept et de l'image acoustique. […] Le lien unifiant le signifiant et le signifié est arbitraire, ou encore, puisque nous entendons par signe le total résultant de l'association d'un signifiant à un signifié, nous pouvons dire plus simplement : le signe linguistique est arbitraire. (Saussure, 1995, p. 99)

Pensons aux signes utilisés en mathématiques, +, par exemple, dont le signifiant ne peut se comprendre sans une relation au signifié. L'opération associe à deux objets de même nature un troisième objet ce cette même nature : 2+3 est égal à 5 portant sur les nombres entiers ou $\vec{u}+\vec{v}=\vec{w}$ où le vecteur somme est défini dans un espace vectoriel. Le signifiant est le même mais les signifiés ne pourront être mis en relation que par la structure sous-jacente des nombres entiers munis de l'addition, ou d'un espace vectoriel sur lequel une addition a été définie.

Peirce rajoute dans sa définition d'un signe un troisième élément, l'interprétant, c'est à dire la compréhension de la relation entre le signifiant et le signifié. Ainsi, pour Peirce, la signification n'est pas une simple relation entre le signifiant et le signifié mais un signe n'a de signification que lorsqu'il est interprété : « *nothing is a sign unless it is interpreted as a sign* » (Peirce, 1931, 2.172). Ainsi, Peirce étend la définition de la sémiologie de la langue à la logique :
Disons que la logique proprement dite est la science formelle des conditions de la vérité des représentations (Peirce, 1931-58, 2.229)
L'élément signifiant (*representamen*) est la partie du signe qui permet de véhiculer la signification ; il est premier au sens où il est indépendant de toute chose. Peirce distingue trois *representamen* :

- le *qualisigne* correspond à une propriété ou une qualité qui fonctionne comme un signe : pour retrouver une couleur, je peux utiliser un objet peint de cette couleur ; l'objet n'a d'importance dans cette situation que par la couleur qu'il porte, c'est cette couleur qui est l'élément porteur de la signification,
- le sinsigne correspond à un signe relié de manière causal à l'objet qu'il représente : la fumée est le signe d'un feu,
- le legisigne correspond à un signe relié conventionnellement, par une règle ou par une loi à l'objet qu'il désigne : le feu rouge signifie qu'il faut s'arrêter au croisement.

Illustration 1: Le code d'Hammurabi

L'objet signifié ou plus exactement certaines propriétés de l'objet signifié sont reliées à l'élément signifiant. Il est second au sens où il est lié à un ou des éléments signifiant. L'objet *détermine* son signe ; c'est à dire, la nature de l'objet contraint la nature du signe en ce qu'elle porte une signification.
Dans l'histoire, il y a de nombreux systèmes de signes qui ont été inventés pour transmettre l'information, pour la conserver et pour la fixer, pour garder trace et faire référence : le code d'Hammurabi en

est un bon exemple ; ce texte, considéré comme un des premiers texte de loi, fixe pour la population les règles à suivre : l'écriture, comme système de signes permet de *fixer* la loi qui ne dépend ainsi plus d'une tradition orale. L'écriture est ainsi un de ces systèmes et son invention est la première grande révolution de l'humanité, selon Serres (2012). Toute écriture est fondée sur l'existence d'un code socialement partagé permettant de regrouper des signes et de transporter et d'arranger les signifiants entre eux. Coder, c'est ainsi construire avec des signes un système préservant à l'intérieur d'un groupe une signification partagée. En écrivant « chat », je partage à travers l'assemblage de signes-véhicules (c, h, a, t) un nouveau signe dont le signifiant réfère à l'animal. En écrivant « tach », j'utilise le même ensemble de signes-véhicules pour construire un signifiant pour une autre communauté, au faite du verlan.

Mathématiques et enseignement

Le langage mathématique utilise des signes et une grammaire permettant de coder des phrases transportant et partageant une signification. La question à laquelle les logiciens se sont confrontés est précisément de savoir s'il est possible de faire des mathématiques uniquement avec la syntaxe, l'assemblage de signes-véhicules. Ou si au contraire, les signes utilisés en mathématiques ne sont pas un support de la pensée :
les grands mathématiciens ont rarement effectué des découvertes importantes en se livrant simplement à une manipulation aveugle des symboles, car les mathématiques ne se situent pas seulement au niveau de la syntaxe, elles véhiculent constamment du sens, des interprétations. (Klein, 2005).
La question n'est-elle pas alors de construire le sens des mathématiques en s'appuyant sur tous les systèmes sémiotiques capables de décrire la pensée mathématique :
Au lieu de tenter de penser le formalisme mathématique comme langue (formelle), il faut à l'inverse, penser la langue (verbale) comme participant de la panoplie d'instruments sémiotiques du travail mathématique. (Chevallard, 1995-96, p.52)

Illustration 2: Magritte, ceci n'est pas une pipe

Depuis de nombreuses années la recherche s'est intéressée aux apports de la sémiotique pour l'enseignement et l'apprentissage des mathématiques. Raymond Duval (1988) a certainement été un des pionniers à introduire des analyses sémiotiques en didactique des mathématiques en s'appuyant sur le concept de registres de représentation sémiotique : ce qui acquiert un caractère prioritaire dans l'enseignement des mathématiques est le couple « système de signe - objet » ; l'appréhension[1] des objets mathématiques ne peut s'entendre qu'à travers certaines de leurs représentations. Travailler avec un objet mathématique impose de travailler avec certaines de ses représentations et, pour parodier Magritte (ci-contre), 1 est différent de un. Ce n'est qu'un signe, parmi d'autres, qui désigne, représente le nombre un, tout comme d'autres symboles, dans d'autres registres peuvent aussi représenter ce même nombre. Contrairement à ce qui se passe dans l'art, les signes en mathématiques se doivent d'être opérationnels, c'est à dire efficients à l'intérieur d'une représentation. Il est toujours possible d'utiliser d'autres symboles, mais la familiarité que l'on a avec les symboles est particulièrement importante pour atteindre à travers eux le sens de l'objet représenté. Un simple décalage dans ces représentations peut rendre difficile des prises de décisions sur des objets pourtant familiers. L'exemple des deux multiplications de la figure 3 illustre bien ce décalage : s'il est assez facile de se convaincre que la première multiplication est juste en vérifiant l'ordre de grandeur, le chiffre des unités, en faisant éventuellement une « preuve par 9 », il est beaucoup plus délicat de savoir si la seconde, écrite en base huit est exacte. Les indices, au sens de Peirce (1978/1938), ne sont plus présents, la contiguïté du signe et de l'objet n'est plus assurée, les traces sensibles du phénomène étudié (ici une multiplication) ne permettent plus l'expression directe de l'objet représenté.

$$\begin{array}{r} 2375 \\ \times \quad 7 \\ \hline 16625 \end{array} \qquad \begin{array}{r} 2375 \\ \times \quad 7 \\ \hline 21353 \end{array}$$
Illustration 3: Deux multiplications... justes !

Les objets mathématiques que les mathématiciens manipulent ont des représentations diverses et le

1 La fin de cette section est repris de Aldon, G. (2012). *Multi-représentations*, Revue en ligne Mathematice, n°32 http://revue.sesamath.net/spip.php?article461 (vu le 30/11/2013)

travail du mathématicien ne se fait pas sur les objets mais sur certaines de leurs représentations : « *Des représentations sémiotiques sont des productions constituées de signes appartenant à un système de représentation qui a ses propres contraintes de signifiance et de fonctionnement. »* (Duval 1991, page 234)

Les objets mathématiques peuvent alors être considérés comme la classe d'équivalence de leurs représentations modulo la relation d'équivalence dans l'ensemble des représentations définie par : deux représentations sont en relation si elles sont des représentations d'un même objet mathématique. Cette remarque a deux conséquences essentielles :

- un objet mathématique peut être maîtrisé dans un contexte et étranger ou difficile dans un autre (c'est ce qu'illustre l'exemple des deux multiplications).
- la conversion d'un registre de représentation à un autre est essentiel pour appréhender un objet mathématique, ce qui demande un travail de traduction qui à la fois fait perdre des éléments de signification mais aussi en rajoute ; en modifiant le signifiant, c'est à dire la façon de désigner l'objet, on modifie, on enrichit on complète le signifié, l'objet désigné.

Codage et secret

Un autre aspect du codage qui rejoint les mathématiques est lié à la cryptographie (voir par exemple Lehning, 2012), c'est à dire la science permettant de coder et transmettre un message dans une communauté sans que l'extérieur ne soit capable de comprendre le sens du message initial.

Ce mot que vous m'avez envoyé hier

soir, je ne peux l'admettre. Il est

vain de tuer ainsi ces affreuses

heures. Soyez sérieux, mon prince.

Shéhérazade.[2]

Dans une histoire de codage, il y a trois personnes : le codeur (Alice), le décodeur (Bob) et le pirate (Carole). Le codeur doit pouvoir chiffrer (encoder, coder, crypter,. . .) facilement son message, le décodeur doit pouvoir le déchiffrer (décoder, décrypter,. . .) facilement et le pirate ne doit pas pouvoir le décoder !

L'utilisation du mot « chiffre » montre bien que le codage va directement être lié à l'utilisation des nombres et à leurs propriétés. Le codage de César, par exemple, qui correspond à un décalage des lettres dans l'alphabet peut être interprété comme une addition modulo 26[3] (en supposant que l'on utilise que les 26 lettres de l'alphabet comme signes-véhicules). Le codage de Vigénère[4], est également construit sur une addition utilisant une « clé » : une fois le message chiffré (en utilisant par exemple le numéro d'ordre de la lettre dans l'alphabet ou le codes ASCII, ou...) on place la clé (elle aussi chiffrée) sous le message et on additionne lettre à lettre modulo 26 ; par exemple, en utilisant la clé « MATHEMATIQUES » :

BONJOUR NOUS AVONS RENDEZ VOUS

deviendra :

2	15	14	10	15	21	18	14	15	21	19	1	22	15	14	19	18	5	14	4	5	26	22	15	21	19	
13	1	20	8	5	13	1	20	9	17	21	5	19	13	1	20	8	5	13	1	20	9	17	21	5	19	
15	16	8	18	20	8	19	8	24	12	14	6	15	2	15	13	26	10	1	5	25	9	13	10	26	12	

Et le message codé, retranscris en lettres devient :

OPHRTHSHXLNF0BOMZJAEYIMJZL

La faiblesse d'un tel codage provient du fait qu'Alice doit préalablement transmettre à Bob la clé !

Les codages modernes reposent sur des propriétés arithmétiques et des fonctions « trappes » : il est facile de trouver l'image d'un nombre (c'est le codage) mais difficile (c'est à dire non réalisable dans un temps suffisamment court) de trouver l'antécédent quand on connaît l'image (c'est le décodage).

2 Lire juste les premiers mots de chaque vers... cité par Lehning, 2012.

3 Calculer modulo 26 revient à calculer avec les restes de la division par 26, c'est à dire les nombres 0, 1, …, 25. Dans ce système, 25+1=0 puisque si j'ajoute deux nombres dont les restes dans la division par 26 sont respectivement 25 et 1, la somme aura comme reste 0 dans la division par 26. Par exemple : 51=1x26+25, 79=3x26+1 et 51+79=130 avec 130=26x5+0.

4 Vigénère (Blaise de, 1523-1596) diplomate, écrivain, alchimiste, traducteur de l'hébreu et du grec ancien et cryptographe, Blaise de Vigénère est un des grands esprits de la Renaissance ; il est l'auteur du Traicté des chiffres ou secretes manières d'escrire, publié chez Abel L'Angellier, au premier pillier de la grand' salle du palais, en 1586. http://gallica.bnf.fr/ark:/12148/bpt6k73371g/f2.image.r=.langFR (consulté le 5 novembre 2013)

Ainsi la clé permettant le codage peut devenir publique mais seul le décodeur connaîtra la clé pour décoder. Il n'y a plus de transmission de clé secrète. C'est sur ce principe que le codage RSA[5] est construit et permet le codage de nos numéros de cartes bancaires sur le web...

Références

Chevallard, Y. (1995-96). *Les outils sémiotiques du travail mathématique,* Petit x, n°42
Duval, R. (1991). Structure du raisonnement déductif et apprentissage de la démonstration. *Educational Studies in Mathematics*, 22-3, 233261.

Klein, E. (2005). *L'efficacité des mathématiques est-elle si déraisonnable ?*, Forum de la théorie, http://www.irem.univ-montp2.fr/L-efficacite-des-mathematiques-est (vu le 31 octobre 2013)
Lehning, H. (2012). *L'univers des codes secrets*, Ixelles éditions, Bruxelles
Peirce, Charles Sanders (1931-58): *Collected Writings* (8 Vols.). (Ed. Charles Hartshorne, Paul Weiss & Arthur W Burks). Cambridge, MA: Harvard University Press
Peirce, C. (1938/1978) *Ecrits sur le signe*, Le Seuil, Paris.

Saussure, F. (1995). *Cours de linguistique générale,* Payot, Paris.
Serres, M. (2012). *Petite Poucette*, Le Pommier

5 Rivest, Shamir et Adelman sont les trois mathématiciens à l'origine de ce système de codage.