

CODAGE, CRYPTOLOGIE ET APPLICATIONS

Bruno Martin, Presses Polytechniques et Universitaires Romandes, Collection Technique et Scientifique des Télécommunications (CTST), Lausanne, 2004, ISBN 2-88074-569-1 — 350p.

*Note de lecture de Jean-Yves Antoine
Mél : Jean-Yves.Antoine@univ-tours.fr*

L'histoire de la cryptographie se confond avec celle des sociétés humaines, ou du moins est-elle née avec l'émergence des grands royaumes et empires antiques. C'est ainsi que toute introduction à la cryptologie prend généralement comme premier exemple illustratif les techniques sommaires de cryptage utilisées par les armées et les agents de César (« chiffre de César »). Dès lors, l'évolution de la cryptologie n'a été qu'une longue compétition entre crypteurs et déchiffreurs. Cette évolution a longtemps eu affaire avec certains champs disciplinaires relevant des sciences cognitives.

Ainsi, les techniques de déchiffrement utilisées à la Renaissance reposaient-elles sur une analyse statistique de la distribution des lettres dans la langue considérée. Ces recherches, qui préfiguraient les développements de la linguistique statistique au XX^e siècle, sont d'ailleurs utilisées — si l'on s'arrête à des principes très généraux — dans les tentatives de déchiffrement des langues anciennes disparues.

De même, il est inutile de rappeler le rôle prééminent — mais souvent occulté — qu'a joué au cours de la seconde guerre mondiale Alan Turing, le père de l'Intelligence Artificielle (voir le fameux « test de Turing »), dans le déchiffrement des codes secrets allemands utilisant la machine ENIGMA.

Turing était avant tout un grand mathématicien et, dès cette époque, la lutte entre cryptage et décodage reposait sur des techniques purement mathématiques. Cette situation perdure à l'heure actuelle, certaines techniques de chiffrement reposant par exemple sur la capacité d'un ordinateur à trouver les diviseurs d'un nombre entier donné.

Il en va de même pour le codage. Moins connue, cette technique consiste à rajouter à un message que l'on souhaite transmettre des informations redondantes (bits de contrôle) pour pouvoir détecter, voire corriger, d'éventuelles erreurs de transmission. Invisibles, ces techniques de codage se retrouvent dans notre vie quotidienne, qu'il s'agisse des transmissions satellitaires, de nos téléphones mobiles ou encore du transit des informations à travers le réseau Internet. Elles constituent, elles aussi, un bel exemple d'applications pratiques de théories mathématiques (espaces vectoriels, applications linéaires, calcul polynomial...) qui n'avaient pas été développées pour elle.

Que le lecteur ne se trompe donc pas : l'ouvrage de Bruno Martin consacré au codage et à la cryptologie présente avant tout les principes mathématiques sous-jacents aux méthodes de codage et de cryptologie. Cette dimension théorique peut

rebuter de prime abord. Il s'agit cependant d'un passage obligé pour qui souhaite atteindre une compréhension réelle de ces techniques.

Tout au long de l'ouvrage, Bruno Martin prend d'ailleurs bien soin de limiter autant que possible le recours à ces notions mathématiques. Lorsqu'elles s'avèrent nécessaires à l'exposé, le chapitre concerné commence alors par de brefs rappels très utiles. Au final, ce livre me semble accessible à toute personne dotée d'un bagage universitaire de premier cycle scientifique. Ceci n'est pas toujours le cas d'autres ouvrages qui multiplient, sans réelle nécessité, l'exposé de théorèmes spécifiques à la portée très restreinte.

En revanche, cet effort salutaire de synthèse va parfois à l'encontre de l'objectif recherché. Prenons un exemple dans la partie consacrée au codage. Ne voulant pas faire appel à trop de pré-requis sur les relations d'équivalences, Bruno Martin présente la méthode de décodage par tableau standard en démontrant que les classes latérales partitionnent bien l'espace de codage. Cette démonstration n'étant pas centrale à la compréhension de la méthode, je crois qu'il aurait été aussi efficace de rappeler, sans le démontrer, le résultat bien connu selon lequel les classes d'une relation d'équivalence partitionnent l'espace sur lequel elles sont définies. Au pire, le lecteur non averti admettra sans peine, éventuellement à l'aide d'un exemple, ce résultat. D'autres exemples montrent qu'il aurait ainsi été possible de présenter d'une manière encore plus limpide certaines notions abordées dans l'ouvrage.

De même, les démonstrations proposées par Bruno Martin sont parfois partielles, l'auteur laissant implicitement au lecteur le soin de les compléter. Cette démarche permet sans aucun doute au lecteur de s'appropriier le sujet. On peut cependant imaginer qu'une personne non spécialiste peut ainsi se retrouver bloquée dans sa compréhension.

En conclusion, Bruno Martin nous propose un texte plus accessible que la moyenne des ouvrages traitant du sujet, mais exigeant tout de même d'être abordé papier et crayon en main ! Cet effort sera récompensé par une compréhension fine et très complète des techniques de codage et cryptologie.

De ce point de vue, j'ai apprécié l'exhaustivité mais également l'effort de synthèse d'un ouvrage qui fait émerger le corpus central des connaissances mises en jeu dans ces domaines, en alliant résultats théoriques, exercices applicatifs ou illustratifs ainsi que de multiples ouvertures précises sur les applications technologiques des notions étudiées. Après un exposé sur les codes polynomiaux, le lecteur retrouve par exemple la liste des polynômes générateurs utilisés actuellement par nos réseaux informatiques locaux ou globaux.

Au total, Bruno Martin nous propose en 350 pages un ouvrage à la fois encyclopédique et synthétique qui n'a pas d'équivalent en français. Par ses qualités, ce livre connaîtra indéniablement une longue carrière. Il me reste donc à espérer que les éditions successives de l'ouvrage seront encore plus accessibles au lecteur non spécialiste, et pourquoi pas aborderont également les techniques récentes de stéganographie (masquage d'information) et de tatouage numérique. Si ces dernières ne sont pas abordées dans cet ouvrage, c'est peut-être qu'il manque encore à la stéganographie de réels fondements mathématiques...

L'auteur de la revue critique



Jean-Yves Antoine est professeur en informatique à l'Université François Rabelais de Tours (laboratoire LI). Après un doctorat sur la compréhension de parole préparé à l'Institut de la Communication Parlée (Grenoble), il a mené des études post-doctorales sur le même thème au CLIPS-IMAG (Grenoble) avant de rejoindre le laboratoire VALORIA (Univ. de Bretagne Sud). Il conduit des travaux sur le dialogue homme-machine, l'aide à la communication pour personnes handicapées, l'évaluation des systèmes d'ingénierie des langues ainsi que des recherches en linguistique de corpus. Il anime un groupe de recherche du PRC-13 sur la compréhension de la langue.

CERVEAU, SEXE ET POUVOIR

Catherine Vidal, Dorothée Benoit-Browaeyns, Belin, Collection Regards sur la Science, 2005, ISBN 2701138582 — 110 p. — 16 €

Note de lecture de Valérie Buron
Mél : valburon@yahoo.fr

Un livre écrit par deux femmes et dont le titre est *Cerveau, Sexe & Pouvoir* peut-il aujourd'hui encore choquer ? Non bien sûr, cela paraît évident pour qui a un peu de bon sens et vit bien au XXI^e siècle. Pas pour Catherine Vidal et Dorothée Benoit-Browaeyns qui, manifestement, ont ressenti le besoin d'écrire 90 pages pour tenter de convaincre un audimat, d'avance convaincu. Est-il besoin de rappeler que les capacités cognitives ne se mesurent pas au poids du cerveau, de quelques grammes plus lourd chez l'homme ? Et que ce n'est pas le nombre de neurones qui compte mais la force de leurs connexions ? Ou bien alors, l'ouvrage vise ceux qui prennent au sérieux des livres comme « *Pourquoi les hommes mentent et les femmes ne savent pas lire une carte routière* » (Pease et Pease, 2002) ; bref, ceux qui ne lisent pas avec un vague sourire sur les lèvres, voire des éclats de rire, ces livres qui, selon les auteurs, sont un joli coup de pub à la Paris-Match. Dans ce cas, l'ouvrage grand public de Catherine Vidal et de Dorothée Benoit-Browaeyns parviendra-t-il à convaincre ? Pas sûr.

Car l'objectif, on l'aura compris, est de traquer les préjugés ancestraux, parmi lesquels, dès la naissance, les femmes ont de grandes capacités pour s'exprimer et les hommes pour s'orienter. Et que cela ne pourra pas évoluer. Contre ces idées reçues, les auteurs usent d'arguments implacables en s'appuyant sur des études parues dans de grandes revues scientifiques internationales. Mais les deux femmes vont plus loin que la question de savoir si le cerveau a un sexe. Et c'est ce qui est réellement intéressant dans cet ouvrage. Elles ont choisi de dénoncer de manière plus générale l'utilisation à mauvais escient de l'apport de la biologie ces dernières années et de tout ce qu'on peut lui faire dire, par, notamment, une lecture sans fondement scientifique des images d'imagerie cérébrale. Elles dénoncent aussi toute l'exploitation commerciale en jeu derrière cette toute dernière technologie scientifique. Par exemple, le soi-disant repérage des zones de notre cerveau susceptibles de nous rendre disponibles lors des plages publicitaires... Un mot a même été créé pour qualifier ce nouveau commerce : « le neuromarketing ». Mais au-delà de la rencontre entre la neurologie et le *marketing*, les deux auteurs expliquent qu'à travers cette association et cette recherche du profit, c'est une évolution de notre système de pensée dans la société qui s'impose petit à petit. Tout ce qui est marqué au fer « neuro » devient potentiellement commercialisable. Car ça marche. Par ailleurs, on appréciera également le bon passage sur la plasticité cérébrale et le rappel — qui devrait en être un — que l'homosexualité (Rice *et al.*, 1999), comme la fidélité (Vidal, 1999), n'est pas une affaire de gènes. Dommage que ces parties n'arrivent pas plus tôt dans le livre.

Alors, finalement, ce livre n'est-il qu'un de plus sur l'éternel débat de l'inné et de l'acquis ? En partie. Et avec un parti pris énoncé clairement : très peu d'inné (pour ne

pas dire « pas ») et beaucoup d'acquis. Mais à l'heure du clonage du premier embryon humain en Corée du Sud, ce livre est le bienvenu et fait la part belle au social. À la possibilité de penser que « tout n'est pas joué » à la naissance. Soulignons qu'enfin, à travers ce livre, c'est aussi une réunion — réussie — de deux compétences, scientifique et journalistique, qui s'exprime. Au fait, si à la question de départ vous avez été tenté de répondre « oui, parce que dans la société, ce sont les hommes qui gouvernent » ou « non, parce que les femmes ont des capacités naturelles pour s'exprimer », dans les deux cas, *Cerveau, Sexe & Pouvoir* est à lire... d'urgence.

Références Bibliographiques

Pease A. et Pease N. (2002). Pourquoi les hommes mentent et les femmes ne savent pas lire une carte routière. First Edition.

Rice G, Anderson C, Risch N, Ebers G. (1999). Male homosexuality: absence of linkage to microsatellite markers at Xq28. *Science*, 284, 665-667.

Vidal C. (1999) Gène de la fidélité ou fidélité à la génétique ? *Le Monde*, Paris, France. 3 septembre 1999.

L'auteur de la revue critique

Valérie Buron est docteur en sciences cognitives. Elle suit actuellement une formation de journaliste scientifique (DESS de journalisme scientifique et technique, Montpellier).

LOGIQUE DE LA CONCEPTION

FIGURES DE SÉMIOTIQUE GÉNÉRALE D'APRÈS CHARLES S. PEIRCE

Bernard Morand, L'Harmattan, Collection L'Ouverture Philosophique, 2004, ISBN 2-7475-6366-9 — 294 p. — 24.50 €

Note de lecture de Joel Revault

Mél : Joel.Revault@univ-ubs.fr

Dans son ouvrage, intitulé *Logique de la conception*, Bernard Morand constate le manque de maturité scientifique du domaine de la conception : les exemples sont légion, mais l'informatique en raison de sa courte histoire et de son omniprésence est particulièrement affectée par ce manque. Outre qu'il s'agit d'un sujet bien connu de l'auteur, le domaine du génie logiciel est de ce fait un laboratoire pertinent d'examen et d'application des processus de conception.

Le premier chapitre recense et commente les étapes et les courants importants dans la pratique de la conception des logiciels. Il montre aussi que l'informatique n'est pas une et inscrite dans le marbre mais, au contraire, plurielle et sujette à de multiples évolutions : ce qui pose de nombreuses questions, dont celle des fondements n'est pas des moindres.

Allons-nous sur le plan conceptuel nous limiter aux propriétés d'une science du strict calcul alors que nos réalisations ont depuis longtemps mis en évidence l'importance du vague, de l'échange, de la répartition des responsabilités et de l'intelligence. Pensons-nous que le cas standard des formulations par un utilisateur d'une question en intention qui conduit un logiciel à nous répondre en termes d'extension puisse exploser ? Quelles sont les conditions de dépassement de ce verrou ? Autrement dit à quand un système répondant en intention du même niveau que son utilisateur et que peut apporter la méta-modélisation dans cette quête ?

Ainsi même si d'immenses progrès ont vu le jour avec l'apparition des systèmes à base de règles, des réseaux sémantiques, des logiques terminologiques (ou de description), des langages unifiés (comme UML), des langages de classes (animant des systèmes à objets), des motifs de conception (ou *design patterns*) et bien d'autres concepts élaborés, il faut bien admettre, avec l'auteur, que nous sommes loin du compte. D'ailleurs l'ouvrage ne dit-il pas que nous ne pourrions l'atteindre qu'en embrassant tout le flot des informations qui permettraient de synthétiser une forme idéale et achevée ?

On en vient alors à s'interroger sur notre façon de penser le monde, de le représenter et de communiquer à son propos. C'est là aborder la question des fondements, ce qui oblige à prendre quelque hauteur. Comme l'indique le sous-titre *Figure de sémiotique générale d'après Charles S. Peirce*, l'auteur va chercher les ressorts indispensables dans la science des signes. Ceci nécessite évidemment de nombreuses explications sur le vocabulaire et surtout sur l'essence des signes selon Peirce. En effet, la pensée de Peirce n'est pas la référence la plus commune en la matière dans les sciences de l'ingénieur, et, même si l'on a bien perçu certaines

impasses de nos activités dans différentes spécialités, le choc peut être douloureux face à la culture scientifique la plus répandue aujourd'hui.

Cependant de nombreuses notions (comme celle d'interprétant, par exemple) se construisent progressivement tout au long de l'ouvrage, si bien que les fragiles échafaudages des premiers pas sont retirés sans crainte, car entre temps notre connaissance s'est étendue en largeur aussi bien qu'en profondeur.

Finalement qu'apprend-on ? Eh bien, cela dépend de nos connaissances préalables en matière de logique, de méthode de conception et de représentation, mais aussi de l'expérience collatérale (ressemblante) du lecteur (récepteur) et de l'auteur (émetteur). Sans prétendre être exhaustif nous y avons personnellement lu : qu'il est plusieurs façons d'abstraire, que toute activité qui prétend se situer hors du temps ou en néglige l'importance est condamnée par avance, que la frontière entre théorie et pratique est infiniment perméable (ce dont nous sommes nous-même absolument convaincu), que le continu et l'infini sont des notions premières alors que le discret et le fini n'en sont que de pâles clichés, que la logique dite des mathématiques n'est pas toute la logique, que le vague ne peut être éradiqué, que l'analyse et la synthèse entretiennent des liens d'entrelacement, que la force d'un signe est dans sa capacité de germination, que le flot informationnel est ce qui donne vie à notre pensée...

De la même façon que les projections binaires d'une authentique relation ternaire ne traduisent pas toute la puissance de celle-ci, chacune des affirmations ci-dessus, prise séparément, ne rend pas compte de l'interprétation globale ou synthétique de notre lecture car celles-ci sont bien souvent étroitement dépendantes. Pour preuve remarquons que la plupart d'entre elles ne sont intelligibles qu'à travers la prise en compte du temps, de l'idée d'infini et de continuité.

Un autre niveau de commentaire amènerait à discuter de chaque terme et du souci de précision qui apparaît tout au long de l'ouvrage, ainsi que de tous les résultats de classification qui en résultent. S'il est vrai que certaines distinctions élémentaires sont reprises (interprétant/interprété), d'autres méritaient effectivement d'être développées à la lumière du mode de pensée retenu (analyse/synthèse) ou revisités dans le contexte (intention/extension). Sur les résultats de classification (la reconnaissance de 66 classes par exemple) ne s'agirait-il pas d'une tentative plus que d'un résultat, ne s'agit-il pas d'y voir une expérience invitant à poursuivre la réflexion, à rester à l'écoute, autant que l'avènement d'une carte pour la lecture des signes ?

Parallèlement à la construction « en l'air de châteaux compliqués » l'ouvrage propose de les « copier sur la terre ferme », c'est-à-dire d'appliquer. Bien sûr les deux actions ne sont pas simultanées car le livre (et non pas seulement ce livre en particulier) est par essence linéaire et l'acte d'écriture ne fournit que des instantanés sur le processus global et évolutif de la pensée, mais l'entrelacement rend bien compte du caractère indissociable des aspects théoriques et pratiques de l'étude.

On en revient donc au génie logiciel qui fait amplement usage de diagrammes dont les notations sont aujourd'hui uniformisées par le langage UML. Le premier objectif est de dépasser l'opposition entre iconoclaste et iconophile, si ce dépassement est nécessaire encore faut-il en trouver les moyens ; c'est le rôle attribué à la notion de ressemblance, notion vague s'il en est. Les ressemblances devraient-on dire car leur émergence nécessite des connaissances, des indices, des moyens de perception, des représentations selon différents points de vue : toutes choses qui ne sont pas obligatoirement partagées (ni partageables) par tous les interprètes des diagrammes.

Ce dépassement passe aussi par la reconnaissance des dissemblances (surtout dans les mouvements de synthèse) qui invitent à poser ou à se poser des questions pertinentes. Nous avons aussi cru comprendre que les modes successifs de représentation utilisés en donnent une forme appauvrie à travers le couple similarité-dissimilarité dans la mesure où le couple ressemblance-dissemblance reste ouvert sur les vecteurs de son émergence alors que nos diagrammes sont verrouillés par la lecture qui doit en être faite *via* des conventions. Ce verrouillage représente à notre avis une technique d'accélération ou de substitution à l'impératif d'expérience collatérale des utilisateurs au sens le plus général.

Certes, malgré cette canalisation sans doute nécessaire, chacun admet aujourd'hui que les langages à base de diagrammes doivent être évolutifs, mais force est de constater que la gestion des évolutions ou des immobilités est gouvernée par des soucis d'un autre ordre au rang desquels les intérêts économiques ont un poids prépondérant.

Concrètement les icônes-diagrammes sont classés en quatre catégories par croisement des caractéristiques de singularité ou possibilité, d'une part, et d'analogie « amalgamante » ou partielle, d'autre part. Les praticiens du génie logiciel reconnaîtront dans les divers diagrammes UML la présence ou l'absence de ces caractéristiques. Nous confirmons l'opinion selon laquelle les diagrammes produits auront en général une double utilisation, l'une pour l'analyse, l'autre pour la synthèse ; nous y voyons la projection de l'entrelacement des deux activités : chacune faisant appel à l'observation, la réalisation de transformations ou manipulations, et le raisonnement.

Dans les exemples, le soin accordé au nommage est fondamental, par exemple la distinction entre patient et malade illustre bien le propos. Négliger ce point annonce des incohérences dans la documentation, des erreurs dans l'exécution, des surprises désagréables dans l'utilisation. Notre pratique du génie logiciel et du développement d'applications nous a maintes fois fourni des exemples de ces incidents en cascades, et inversement elle nous a montré le bénéfice qu'apportent la rigueur et la précision en la matière.

Un dernier point nous a semblé important, il concerne les trois types d'inférences utilisées : la déduction, l'induction et l'abduction. D'où nous viennent ces modes de raisonnement ? De la logique certainement, ce qu'on pourrait appeler le « bon sens ». Quel rapport avec les logiques « dites des mathématiques » qui mettent en avant la déduction, certaines formes d'induction et très rarement l'abduction. Les mathématiciens seraient-ils ceux qui sont dépourvus de « bon sens » ? Pour notre part nous n'en croyons rien. Bien au contraire, notre opinion est que l'usage de l'abduction y est permanent, mais hélas, il n'apparaît que rarement dans l'exposé des solutions aux problèmes mathématiques, on le trouverait pourtant dans la genèse des questions posées.

Nous avons donc été particulièrement intéressé par le (trop) court développement sur le raisonnement abductif. En effet, le raisonnement abductif est une pratique quotidienne dans, par exemple, l'enquête policière, le diagnostic médical (ou autre), l'expertise, la recherche scientifique comme mécanisme de déconstruction même s'il est souvent masqué par la reconstruction qui le suit (la reconstitution du crime) et qui nous laisse croire une fois de plus au règne du raisonnement déductif. Nous terminons sur ce point, en ajoutant, que l'abduction est à mettre en relation avec le vague, l'incertitude endiguée, l'erreur assumée et nombre d'autres questions très actuelles liées entre autres à l'extraction de sens dans les grands ensembles de

données. Il me semble que cette interprétation de l'ouvrage de Bernard Morand prouve s'il en était besoin qu'il s'agit d'une invitation à la réflexion et à l'expérimentation.

L'auteur de la revue critique

Joël Révault est maître de conférences en Informatique à l'Université de Bretagne Sud, il enseigne aujourd'hui le génie logiciel, la logique et les bases de données. Il a auparavant enseigné les mathématiques dans le secondaire, puis la théorie des graphes, la théorie des langages, des éléments d'intelligence artificielle notamment en IUT et en IUP informatique.

Son mémoire de thèse traitait de la modélisation du temps, son travail de recherche actuel concerne l'exploitation des ressources dans les grands ensembles de données.