Antoine Lobstein

CR1, LTCI, **ex-UMR 5141** (O. Cappé)

2 septembre 2016

Rapport à 5 semestres
septembre 2016

1 Curriculum Vitæ

Antoine LOBSTEIN

né le 16 juin 1958 (âge : 58 ans),

nationalité française.

Domicile : 12 rue de la Maison Blanche, 75013 PARIS.

ETUDES ET DIPLOMES :

Baccalauréat Série C, Mention Bien, Strasbourg, **1976**.

Classes préparatoires (Mathématiques Supérieures et Mathématiques Spéciales Section M'), Strasbourg, **1976–78**.

Ingénieur de l'Ecole Nationale Supérieure des Télécommunications (ENST), Paris, **1981**.

DEA de Mathématiques Pures, Mention Bien, Université Paris 6, **1982**.

Thèse de Docteur-Ingénieur de l'ENST, sous la direction du Professeur Gérard Cohen (Bourse du Ministère de l'Industrie et de la Recherche). Titre : *Contributions au codage combinatoire : ordres additifs, rayon de recouvrement*, **1985**.

Habilitation à Diriger des Recherches, Université Paris 6, UFR d'Informatique. Titre : *Contributions combinatoires au codage, en connexion avec la complexité et la cryptographie*, **2002**.

EMPLOIS :

A l'ENST, vacataire du CNRS, mars – août **1985**.

Bourse post-doctorale à l'Université de Technologie de Eindhoven (Pays-Bas), Département de Mathématiques et Informatique du Professeur van Lint, novembre **1985** – février **1986**.

Ingénieur au Service d'Etudes communes des Postes et Télécommunications, Division Paiement Electronique et Monétique, Caen, mars **1986** – juillet **1987**.

Chargé de Recherche de 2ème Classe au CNRS, URA 820 (ENST), dir. M. Claude Gueguen puis M. Jean-Pierre Tubach, devenue UMR 5141 (Télécom ParisTech), dir. M. Henri Maître puis M. Olivier Cappé, à partir de juillet **1987**.
Chargé de Recherche de 1ère Classe depuis le 1er octobre **1990**.

27 mai 2016 : fin de l'UMR 5141, mutation dans un laboratoire non encore fixé.

DIVERS :

Langues pratiquées :

Anglais, espagnol courants.

Séjours :

A l'Institut des Problèmes de Transmission de l'Information, Moscou (Russie), 22 juillet – 4 septembre 1992.
A l'Université de Turku (Finlande), 19 – 30 septembre 1994.
A l'Institut Sobolev de Mathématiques, Novosibirsk (Russie), 31 août – 30 septembre 1999.
A l'Université de Turku (Finlande), 6 – 13 octobre 2001.
Dans le Laboratoire Leibniz de Grenoble, 15 – 19 décembre 2003.

2 Recherche scientifique

2.1 Préambule

Le laboratoire où j'ai travaillé depuis mon entrée au CNRS en 1987, le LTCI (Laboratoire de Traitement et Communication de l'Information), a été mis en FRE en janvier 2016, puis désassocié du CNRS en mai 2016. En conséquence, son personnel CNRS doit quitter le LTCI avant la fin de l'année civile.

Mon laboratoire d'accueil n'est pas encore fixé. Il m'est donc un peu difficile de faire des projets clairs sur la période à venir, même si j'ai encore encore des plans en cours avec l'un de mes collègues du LTCI.

2.2 Activités passées : présentation générale

Ma problématique peut s'énoncer de manière très générale de la manière suivante : on se place dans un **espace discret** (espace vectoriel de Hamming sur un corps fini, anneau d'entiers, graphe, ...) muni d'une distance, et on étudie certaines propriétés de certains sous-ensembles (appelés *codes*) de cet espace, propriétés relatives à une distance fixée. En général, on cherche des codes ayant une certaine propriété, et dont la taille soit la plus **petite** ou la plus **grande** possible, selon les cas.

Depuis quelques années, j'ai ainsi travaillé sur le thème des *codes identifiant des sommets, ou des ensembles de sommets, dans un graphe*, thème qui a connu un développement certain dans la communauté des Mathématiques Discrètes : plusieurs colloques centrés sur ce sujet réunissant une soixantaine de chercheurs, environ 350 articles parus pendant ces vingt dernières années, ... Une bibliographie, que je mets à jour autant que possible, est d'ailleurs accessible en ligne sur mon site.

En collaboration avec des chercheurs de plusieurs institutions et pays : Gérard Cohen (LTCI), Iiro Honkala (Univ. de Turku, Finlande), Gilles Zémor (Univ. de Bordeaux), Irène Charon (LTCI, maintenant Professeur Emérite), Olivier Hudry (LTCI), Nathalie Bertrand (CNRS), Emmanuel Charbit (stagiaire à TPT), et David Auger (Univ. de Versailles Saint-Quentin-en-Yvelines), ainsi que Sylvain Gravier, Michel Mollard et Julien Moncel (Laboratoire Leibniz du CNRS à Grenoble), et Yael Ben-Haim (Univ. de Tel-Aviv), cette thématique de type combinatoire a déjà donné naissance à de nombreux articles et communications.

La variante de base du problème de départ est la suivante : étant donné un graphe $G = (V, E)$, muni de la distance du plus court chemin, un ensemble (appelé *code*) de sommets $C \subseteq V$ est dit *t-identifiant* si, pour un sommet $v \in V$, la donnée des mots de code qui en sont à distance au plus t caractérise ce sommet de manière unique.

Cette appproche permet de modéliser la recherche et la détection de pannes dans un réseau dans lequel certains nœuds (les mots de code) sont capables de signaler un dysfonctionnement dans leur voisinage, sans pour autant pouvoir indiquer exactement où. La détection de fumée dans un bâtiment, dont le plan est représenté par un graphe, peut également suivre ce modèle. En effet, si les détecteurs sont placés sur les sommets correspondant à un code identifiant, alors le seul fait de savoir quels détecteurs ont signalé un problème parmi les sommets qui leur sont voisins permet de localiser le sommet problématique.

Si l'on choisit pour graphe G le cube n-dimensionnel, on a un problème assez proche des problématiques liées au rayon de recouvrement des codes en blocs, qui a constitué pendant longtemps l'un de mes sujets de recherche (et aussi celui de plusieurs autres chercheurs qui étudient maintenant les codes identifiants).

Toutes sortes de problèmes, relevant de la théorie des graphes, de la complexité, de l'algorithmique ou même de la théorie de l'information, peuvent se poser à partir de cette définition de base :

(i) Un problème survenant naturellement est que l'on désire utiliser **le plus petit nombre** possible de détecteurs ; d'où la recherche des codes identifiants de taille la plus petite possible (= *codes optimaux*) dans différents graphes. On peut aussi s'intéresser au nombre et à la structure propre des codes optimaux, afin d'avoir un choix dans la disposition optimale des détecteurs, et pouvoir procéder plus facilement en cas de remplacement.

(ii) Examen de **familles particulières** de graphes (chaînes, cycles, arbres, graphes planaires, cube n-dimensionnel, grilles, soleils complets, ...).

(iii) Etant donné un graphe G_1 auquel on va, disons, *retirer* un sommet, ou une arête, pour obtenir un nouveau graphe G_2, que peut-on dire de la taille des plus petits codes t-identifiants, s'ils existent, dans les deux graphes G_1 et G_2 ? Les réponses varient en fonction du paramètre t, mais

il existe des paires de graphes, différant par un seul sommet ou une seule arête, avec de grandes variations de taille entre le plus petit code t-identifiant de l'un et le plus petit code t-identifiant de l'autre : si n est le nombre de sommets de l'un ou l'autre graphe, ces tailles peuvent ainsi passer de l'ordre d'une fraction de n à une valeur de l'ordre de $\log_2 n$. Si l'on reprend le modèle d'un bâtiment à protéger avec des détecteurs de fumée, en fermant simplement un couloir (= arête enlevée) ou une salle (= sommet enlevé), on peut donc, dans des cas favorables, économiser un grand nombre de détecteurs/mots de code.

(iv) Une autre manière d'économiser des détecteurs est de modifier leurs pouvoirs : au lieu de surveiller **tous** les sommets à l'intérieur de leur t-voisinage, on décide qu'ils n'en observeront qu'un **sous-ensemble** choisi. Nous parlons alors de *système de contrôle*, notion plus souple, plus puissante mais aussi plus complexe à étudier. Des graphes à n sommets existent, tels que leur plus petit code identifiant ait une taille proche de n, alors que leur plus petit système de contrôle a une taille de l'ordre de $\log_2 n$.

(v) Comme souvent pour des problèmes de graphes, on se pose la question de leur **complexité**, et cet aspect est celui qui a été le plus fortement développé dans nos recherches récentes.

Ces cinq angles d'attaque sont ceux que j'ai développés récemment, mais d'autres sont possibles, qui ont été étudiés plus anciennement et pourraient dans certains cas être réétudiés :

– l'identification *adaptative*, où l'on cherche toujours à reconnaître un sommet par ses voisins mots de code, mais ce de manière progressive, dans une sorte de Mastermind où les réponses reçues vont influencer les questions suivantes : ici, une question consiste à interroger un détecteur pour savoir s'il détecte une panne dans son voisinage, sa réponse sera Oui ou Non, et on peut alors interroger un autre détecteur **en fonction de cette réponse**, alors que le cas non-adaptatif peut être vu comme le cas où l'on pose toutes les questions au début, **d'un seul coup** ;

– l'étude des valeurs que peuvent prendre, dans un graphe identifiable, certains **paramètres classiques** en théorie des graphes, tels que : nombre d'arêtes, degré maximum ou minimum, taille de la plus grande clique, rayon, diamètre, taille du plus grand stable, ... ;

– l'étude des graphes *bipartis* (où il n'y a d'arêtes qu'entre deux sous-ensembles de sommets A et B partitionnant V), dans lesquels on identifie les sommets de la partie A du graphe avec des mots de code choisis exclusivement dans la partie B. On parle alors de codes *discriminants*. C'est en fait une **généralisation** des codes identifiants, car à partir d'un graphe G on peut construire un graphe biparti G^* de manière que << code identifiant dans G >> équivale à << code discriminant dans G^* >>.

2.3 Activités et production spécifiques des 5 derniers semestres

Les thèmes numérotés **(i)** à **(v)** ci-dessus ont été explorés entre 2014 et 2016.

On a abordé les thèmes **(i)** de la plus petite taille possible d'un code identifiant et **(ii)** de certaines familles de graphes, de la manière suivante : en 2014, une conjecture a été posée sur la taille des codes identifiants optimaux dans la famille des soleils complets, qui font partie de la classe plus vaste des "split graphs" ; non seulement nous avons déterminé cette taille, mais nous avons caractérisé et compté tous les codes optimaux, et de plus étendu cette étude à une autre variante proche des codes identifiants, celle des codes *localisateurs-dominateurs* (Publication [**G**] ci-dessous, à paraître).

Le thème **(iii)** d'ajout de sommet ou d'arête a donné lieu à deux publications, dont une en 2014. Dans celle-ci, on voit une différence de comportement des codes t-identifiants selon que $t = 1$, $t = 2$, $t \in \{3, 4\}$ et $t \geq 5$ (Publication [**B**]).

Pour le thème **(iv)** des systèmes de contrôle, nous avons caractérisé les graphes qui atteignent la borne supérieure du plus petit nombre de contrôleurs nécessaire, c'est-à-dire que nous décrivons les "mauvais" graphes, ceux qui ont besoin d'un grand nombre de contrôleurs (Publication [**A**]).

Sur la période écoulée 2015–2016, c'est le thème mentionné en **(i)** de l'étude de la structure des codes optimaux, et notamment de leur nombre, qui a été la plus productive, avec trois articles parus sur cette période. On y contruit notamment une infinité de graphes connectés à n sommets admettant $2^{0,77003\,n}$ différents codes 1-identifiants optimaux, ainsi qu'une infinité de graphes connectés à n sommets admettant $2^{\frac{1+\log_2 5}{5}\,n-\varepsilon}$ différents codes t-identifiants optimaux, $t \geq 1$, $\varepsilon > 0$. (Publications [**C**], [**D**], [**E**]).

Enfin le thème **(v)** de la complexité est celui qui s'est le plus développé sur les derniers mois, et nous avons été amenés à nous pencher sur des classes de complexité autres que les "grandes" classes telles que P, NP, NP-C ou co-NP, mais aussi P^{NP} et L^{NP}, qui contiennent les problèmes de décision qu'on peut résoudre en faisant appel un nombre polynomial (respectivement, logarithmique) de fois à un algorithme résolvant un problème approprié appartenant à NP (polynomial et logarithmique réfèrent à la taille de l'instance) ; et DP, la classe des langages (ou problèmes) L tels qu'il existe deux langages $L_1 \in NP$ et $L_2 \in$ co-NP vérifiant $L = L_1 \cap L_2$. Nous avons un article paru [**F**], un autre sur le point d'être soumis, et de la matière pour trois ou quatre en cours d'élaboration, ne touchant pas tous aux problèmes de domination, de localisation-domination et d'identifcation, mais élargissant notre recherche vers d'autres problèmes classiques de graphes.

Par rapport à ce qui était annoncé dans mon Rapport à 10 semestres de janvier 2014, dans la Section 6 Objectifs, l'étude structurelle de l'ensemble et du nombre de codes identifiants optimaux a été menée à bien et a donné lieu à publications.

2.4 Interactions au sein de mon équipe

Dans ma future ex-équipe, l'ex-UMR 5141, je faisais partie de l'équipe << Mathématiques de l'Information, des Communications et du Calcul >> (MIC^2), incluse dans le Département << Informatique et Réseaux >> de TPT, Grande Ecole formant des ingénieurs en Télécommunications.

De manière peu surprenante, trois membres de cette équipe (Irène Charon —partie à la retraite en juin 2011—, Gérard Cohen—qui part à la retraite cette année— et Olivier Hudry, qui est plus jeune que moi) ont des thèmes de recherche recoupant assez largement les miens (algèbre, théorie du codage, théorie des graphes, combinatoire, complexité, mathématiques discrètes), et d'ailleurs nous avons collaboré ou collaborons très régulièrement, comme peut en attester ma liste de publications.

S'y est ajouté temporairement un thésard à TPT, David Auger (directeur de thèse : Olivier Hudry), qui s'est rapidement intgré à l'équipe, et a co-signé plusieurs articles ; ses qualités d'enseignant-chercheur lui ont ensuite permis de devenir Maître de Conférences à l'Université de Versailles Saint-Quentin-en-Yvelines.

Je continue à travailler avec Olivier Hudry, et nous avons plusieurs projets en cours ; mon départ du LTCI ne devrait pas interrompre cette collaboration, tout en espérant que d'autres puissent se nouer dans mon prochain laboratoire, quel qu'il soit.

2.5 Production scientifique entre janvier 2014 et septembre 2016

Je donne ci-dessous la liste de mes publications depuis janvier 2014, **toutes dans des revues avec comité de lecture** : 6 parues, une à paraître. Entre crochets, je les ai numérotées de 1 à 3, selon l'ordre (décroissant) d'importance que je leur accorde du point de vue de leur apport au domaine de recherche concerné, et de leur impact (impact supposé lorsqu'il s'agit d'un article à paraître).

A [2] David AUGER, Irène CHARON, Olivier HUDRY & Antoine LOBSTEIN, Maximum Size of a Minimum Watching System and the Graphs Achieving the Bound. *Discrete Applied Mathematics*, Vol. 164, pp. 20–33, 2014.

B [2] Irène CHARON, Iiro HONKALA, Olivier HUDRY & Antoine LOBSTEIN, Minimum Sizes of Identifying Codes in Graphs Differing by One Edge. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences*, Vol. 6, pp. 157–170, 2014.

C [1] Iiro HONKALA, Olivier HUDRY & Antoine LOBSTEIN, On the Number of Optimal Identifying Codes in a Twin-Free Graph. *Discrete Applied Mathematics*, Vol. 180, pp. 111-119, 2015.

D [2] Iiro HONKALA, Olivier HUDRY & Antoine LOBSTEIN, On the Ensemble of Optimal Dominating and Locating-Dominating Codes in a Graph. *Information Processing Letters*, Vol. 115, pp. 699–702, 2015.

E [1] Iiro HONKALA, Olivier HUDRY & Antoine LOBSTEIN, On the Ensemble of Optimal Identifying Codes in a Twin-Free Graph. *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences*, Vol. 8, pp. 139–153, 2016.

F [1] Olivier HUDRY & Antoine LOBSTEIN, More Results on the Complexity of Identifying Problems in Graphs. *Theoretical Computer Science*, Vol. 626, pp. 1–12, 2016.

G [3] Olivier HUDRY & Antoine LOBSTEIN, Some Results about a Conjecture on Identifying Codes in Complete Suns. *International Transactions in Operational Research*, à paraître.

2.6 Autres activités

Evaluations :

Entre janvier 2014 et septembre 2016, j'ai été sollicité 5 fois pour des rapports d'évaluation d'articles soumis aux revues spécialisées suivantes :

Australasian Journal of Combinatorics (1 fois),
Advances in Mathematics of Communications (1 fois),
Discrete Mathematics (1 fois),
Electronic Journal of Combinatorics (2 fois).

2.7 Mutation, objectifs, projet de recherche

Comme je l'ai déjà mentionné, le changement de laboratoire que je vais être amené à effectuer ne facilite pas la prospective. Néanmoins, toujours dans le cadre des codes identifiants et de certaines de leurs variantes (codes *localisateurs-dominateurs*, codes *dominateurs*, *systèmes de contrôle*), nous envisageons à moyen terme une comparaison fine des performances de tous ces sous-ensembles de l'ensemble des sommets du graphe.

À plus court terme, nous sommes en train d'approfondir notre étude de la hiérarchie polynomiale des classes de complexité, en vue de faire apparaître des liens nouveaux entre problèmes de satisfiabilité Booléenne et problèmes de graphes.

En plus de tout ceci, d'autres pistes que nous n'imaginons pas encore surgiront inévitablement au cours des prochaines années, surtout lorsque j'aurai été amené à changer d'équipe et à côtoyer des chercheurs aux thématiques différentes.

En tout état de cause, mes activités de recherche devraient donc continuer à s'inscrire dans un cadre fort de Théorie des Graphes en lien avec la Complexité. Si je reprends la conclusion de mon Rapport de 2014 :

“Je souhaiterais d’ailleurs parvenir à élargir encore l’ensemble des personnes avec qui je travaille, soit à l’intérieur de Télécom ParisTech, soit à l’extérieur : pour moi, la recherche signifie la coopération et l’ouverture.”

l’occasion de le faire me sera probablement donnée lors de ma mutation.

3 Enseignement, formation et diffusion de la culture scientifique

Membre du Comité Scientifique de la conférence << Cologne-Twente Workshop on Graphs and Combinatorial Optimization >> (CTW 2014).

4 Transfert technologique, relations industrielles et valorisation

5 Encadrement, animation et management de la recherche