50 ans de problèmes de spectre en logique

Malika More

Exemple introductif

Un *graphe* est une structure constituée par un ensemble n d'éléments appelés *sommets,* dont certains couples sont reliés par des flèches appelées des *arcs.* Le paramètre qui va nous intéresser ici est le *nombre de sommets* d'un graphe donné. Considérons la propriété suivante : *De tout sommet x du graphe part un unique arc, vers un seul autre sommet y, d'où part également un unique arc, vers le sommet x de départ*. Pour un graphe donné, cette propriété est vraie ou fausse. Fixons un nombre de sommets, disons n, et demandons-nous si on peut trouver un graphe à n sommets pour lequel la propriété ci-dessus est vraie. Dans le cas présent, la réponse est : si n est impair, c'est impossible, si n est pair, un tel graphe peut exister.

Définition

D'une façon générale, on se donne une propriété φ (formellement, un énoncé du premier ordre), et on considère l'ensemble des entiers n tels qu'on peut trouver une structure à n éléments pour lequel la propriété φ est vraie : cet ensemble d'entiers s'appelle le spectre de φ.

Dans notre exemple, le spectre de la propriété ci-dessus est l'ensemble des nombres pairs. Depuis les années 1950 jusqu'à aujourd'hui, les publications sur les spectres sont restées occasionnelles, mais jamais complètement absentes, et certaines ont eu un impact considérable. On présente ici un tour d'horizon rapide des questions principales et des résultats les plus importants du domaine ; voir l'article [DJMM], en cours de redaction en collaboration avec Durand, Jones et Makowsky.

Contexte historique

La notion de spectre d'un énoncé a été introduite par Scholz en 1952, dans une courte note où il demande une caractérisation des ensembles d'entiers qui sont des spectres [Sch52]. Or un des centres d'intérêt principaux des logiciens de cette époque est un ensemble de résultats d'*indécidabilité* pour la logique du premier ordre. En particulier, Trakhtenbrot a montré en 1950 qu'il ne peut exister aucune méthode générale permettant de savoir à coup sûr s'il existe une structure n pour laquelle un énoncé donné est vrai [Tra50]. En d'autres termes, la propriété "être un énoncé dont le spectre est non vide" est indécidable. Au vu de cette barrière, Scholz se demande alors ce qu'on peut dire à propos des spectres. Sa question a reçu une réponse étonnante dans les années 70, qui a fait basculer les recherches sur les spectres du champ de la logique mathématique vers celui de l'informatique théorique, nous y reviendrons.

Dans les années 50 et 60, quelques articles tentent de caractériser les spectres par les méthodes de récursivité et d'arithmétique alors en vogue, mais les résultats obtenus ne sont pas convaincants - partiels, trop compliqués ou peu naturels. Toutefois, ces travaux permettent de s'apercevoir que la classe des spectres est très vaste, puisque la quasi-totalité des ensembles classiques issus de l'arithmétique, comme l'ensemble des puissances de 2, l'ensemble des nombres de Fibonacci, etc., sont des spectres. Par ailleurs, s'il est facile de combiner des spectres par des opérations de réunion et d'intersection, l'opération de complément semble plus difficile à effectuer dans le cas général. La question a été posée par Asser en 1955 : le complémentaire d'un spectre ***S*** (c'est-a-dire l'ensemble des entiers qui ne sont pas dans l'ensemble ***S***) est-il forcément encore un spectre [Ass55] ? On ne sait toujours pas y répondre aujourd'hui, et on va voir qu'elle est en fait liée à l'un des problèmes les plus fondamentaux de l'informatique moderne.

Il reste à introduire une dernière question importante à propos des spectres, qui a été formalisée, plus tardivement que les deux autres, par Fagin en 1975. Dans le cas d'un graphe, on peut considérer les arcs comme un ensemble de couples, c'est-à-dire une relation binaire (ou d'*arité* 2) sur l'ensemble des sommets. Une relation d'*arité* 3 est un ensemble de triplets, etc. Un *vocabulaire* est un ensemble de relations de diverses arités. Il semble raisonnable de penser que des énoncés utilisant un vocabulaire riche permettent de définir des spectres plus élaborés que ceux n'utilisant qu'un vocabulaire simple comme celui des graphes (à savoir une seule relation, d'arité 2). Voici un exemple à l'appui de cette intuition. D'après un théorème d'algèbre bien connu, le nombre d'éléments d'un corps *n* est obligatoirement une puissance d'un nombre premier. Réciproquement, étant donnée une puissance d'un nombre premier, on sait construire un corps qui a précisément ce nombre d'éléments. Une axiomatisation de la structure de corps fournit un énoncé (utilisant un vocabulaire constitué de deux fonctions binaires) dont le spectre est l'*ensemble des puissances de nombres premiers*, un objet bien plus compliqué que notre premier exemple (l'ensemble des nombres pairs), qui était le spectre d'un énoncé du vocabulaire des graphes.

On ne trouve pas facilement un énoncé utilisant le vocabulaire des graphes dont le spectre soit l'ensemble des puissances des nombres premiers, mais il en existe pourtant un (assez compliqué).

La question de Fagin est alors bien naturelle : existe-t-il des spectres qu'on ne peut pas définir à l'aide d'un énoncé utilisant le vocabulaire des graphes [Fag75] ? Cette question, et d'autres similaires, sont actuellement toujours ouvertes.

Un changement de point de vue

C'est seulement en 1972, après l'émergence de la notion de modèle de calcul à ressources bornées à la fin des années 60, que Jones et Selman apportent finalement une réponse remarquable et inattendue à la question de Scholz [JS72]. Leur résultat caractérise les spectres comme les *ensembles d'entiers reconnaissables par une machine de Turing non-déterministe* (objet abstrait modélisant la notion d'ordinateur massivement parallèle et conçu bien avant qu'ils existent réellement) *en temps exponentiel*. Il est intéressant de noter que l'apparition des outils conceptuels adaptés a aussi été suivie par deux autres preuves indépendantes et quasi simultanées de ce résultat [Fag74, Chr74].

La correspondance ainsi mise à jour entre les ressources (temps de calcul, mémoire de stockage) utilisées par un algorithme qui *résout* un problème et la forme (syntaxe) d'un énoncé qui *décrit* ce problème est une notion très importante, à l'origine d'un vaste champ de recherche appelé la *complexité descriptive*. Au-delà de la notion de spectres, à la suite de l'article de 1974 de Fagin [Fag74], il s'agit plus généralement de rechercher des équivalents logiques des diverses classes de complexité [Imm99]. L'intérêt de tels travaux est par exemple de fournir des objets robustes, puisque indépendants des détails des modèles de calcul utilisés. A cette occasion, on observe un total changement de perspective : en effet, à l'origine, la logique était l'objet d'étude et la théorie de la complexité en était l'outil, alors que maintenant ces positions sont permutées.

Avec ce nouveau point de vue sur les spectres, on peut revenir à la question posée en 1955 par Asser sur la clôture des spectres par complément pour éclairer en quoi il n'est finalement pas étonnant qu'elle n'ait pas été résolue depuis plus de 50 ans : on peut montrer qu'une réponse négative aurait pour conséquence que $P \neq NP$, résultat dont l'obtention serait récompensée d'un prix d'un million de dollars par le Clay Mathematics Institute.

Exemples de recherches récentes

Le résultat de Jones et Selman a été raffiné par la suite de diverses façons. En particulier, Grandjean a mis a jour une correspondance précise entre le nombre de quantificateurs universels (c'est-à-dire de signes $\forall$) des énoncés d'une part, et le temps de calcul des algorithmes, d'autre part [Gra85, Gra90].

Concernant les questions de vocabulaires, il a été montre par Durand, Fagin et Loescher [DFL98] qu'un vocabulaire constitué de deux fonctions à une seule variable permet de définir des spectres qui sont, dans un certain sens, aussi compliqués que le cas général : c'est ce qu'on appelle un théorème de transfert, il en existe beaucoup d'autres. Au contraire, un vocabulaire constitué d'une seule fonction à une variable ne permet de définir que des spectres très réguliers (comme l'ensemble des nombres pairs) [DFL98]. Récemment, Hunter a relié la séparation de certaines classes de spectres avec des propriétés de clôture de ces classes par des fonctions sous-diagonales [Hun03]. Par exemple, le spectre d'un énoncé utilisant un vocabulaire constitué de plusieurs relations d'arité 2 est forcément aussi le spectre d'un énoncé n'utilisant que le vocabulaire des graphes si et seulement si pour tout spectre S d'un énoncé utilisant le vocabulaire des graphes, l'ensemble $S' = \{ \lceil n/2 \rceil : n \in S \}$ est aussi un spectre du même type (ou [x] représente la partie entière de x).

Conclusion

La question de Scholz a connu des développements surprenants et l'évolution des angles d'attaque des problèmes de spectres a reflété les façons de penser de chaque époque.

Aujourd'hui, les spectres sont devenus une des déclinaisons de la complexité descriptive, sur laquelle ils apportent un éclairage original, et à laquelle ils pourraient bien permettre de nouvelles avancées.

Références

[Ass55] Günter Asser. Das Repräsentenproblem in Prädikatenkalkül der ersten Stufe mit Identität. Zeitschrift für mathematische Logik und Grundlagen der Mathematik, 1 :252{263, 1955.

[Chr74] Claude A. Christen. Spektralproblem und Komplexitütstheorie. PhD thesis, Eidgenössische Technische Hochschule (ETH), Zürich, Switzerland, 1974.

[DFL98] Arnaud Durand, Ronald Fagin, and Bernd Loescher. Spectra with only unary function symbols. In Mogens Nielsen and Wolfgang Thomas, editors, Computer Science Logic, 11th International Workshop, CSL'97, Annual Conference of the EACSL, Aarhus, Denmark, August 23-29, 1997, Selected Papers, volume 1414 of Lecture Notes in Computer Science, pages 189{202. Springer, 1998.

[DJMM] Arnaud Durand, Neil D. Jones, Johann Makowsky, and Malika More. Fifty years of the spectrum problem : survey and new results. En preparation.

[Fag74] Ronald Fagin. Generalized rst-order spectra and polynomial-time recognizable sets. In Richard M. Karp, editor, Complexity of computation (Proc. SIAM-AMS Sympos. Appl. Math., New York, 1973), volume 7 of SIAM-AMS Proceedings, pages 43{73, Providence, R.I., 1974. American Mathematical Society.

[Fag75] Ronald Fagin. A spectrum hierarchy. Zeitschrift für mathematische Logik und Grundlagen der Mathematik, 21 :123{134, 1975.

[Gra85] Etienne Grandjean. Universal quantiers and time complexity of random access machines. Mathematical Systems Theory, 18(2) :171{187, 1985.

[Gra90] Etienne Grandjean. First-order spectra with one variable. Journal of Computer and System Sciences, 40(2) :136{153, 1990.

[Hun03] Aaron Hunter. Spectrum hierarchies and subdiagonal functions. In 18th International Symposium on Logic in Computer Science (LICS'03), pages 281{290. IEEE Press, 2003.

[Imm99] Neil Immerman. Descriptive Complexity. Graduate Texts in Computer Science. Springer, 1999.

[JS72] Neil D. Jones and Alan L. Selman. Turing machines and the spectra of rst-order formulas with
equality. In Conference Record, Fourth Annual ACM Symposium on Theory of Computing, 1-3 May 1972, Denver, Colorado, USA, pages 157{167, New York, NY, USA, 1972. ACM Press.

[Sch52] Heinrich Scholz. Ein ungelöstes Problem in der symbolischen Logik. Journal of Symbolic Logic, 17 :160, 1952.

[Tra50] Boris A. Trakhtenbrot. Impossibility of an algorithm for the decision problem in nite classes. Doklady Akademii Nauk SSSR, 70 :569{572, 1950.