Dérandomisation et méta-complexité

Proposition de sujet de thèse

LIPN, Université Sorbonne Paris Nord, Villetaneuse
Début : septembre 2026
Doctorante : Micol Giacomin
Encadrant : Sylvain Perifel

Micol Giacomin effectuerait cette thèse au sein de l'équipe LoCal du LIPN à l'université Sorbonne Paris Nord à Villetaneuse (93), sous la direction de Sylvain Perifel (professeur des universités). La date prévisionnelle de début est fixée au 1er septembre 2026.

Contexte scientifique

Cette thèse explorera deux aspects duaux de la complexité algorithmique : la méta-complexité d'une part, et d'autre part les bornes inférieures non uniformes et leurs liens avec la dérandomisation.

Méta-complexité La méta-complexité est l'étude de problèmes qui portent eux-mêmes sur la complexité. Par exemple, le problème MCSP (Minimum Circuit Size Problem) a pour entrée un circuit booléen C et un entier s, et doit décider s'il existe un circuit D équivalent à C mais de taille inférieure à s. En quelque sorte, on étudie donc les bornes inférieures sur les circuits du côté algorithmique. Le problème MCSP est bien entendu dans NP, mais sa difficulté reste ouverte. Évidemment, plutôt qu'à la taille des circuits, nous pourrions aussi nous intéresser à d'autres mesures de complexité, par exemple la complexité de Kolmogorov, avec de même le problème de calculer la complexité d'un mot donné en entrée.

Ce domaine est devenu très actif récemment, notamment par sa capacité à tisser des liens entre différentes questions. Par exemple, Liu et Pass [LP20 ; LP22b] montrent que l'existence de fonctions à sens unique est équivalente à la difficulté de calculer la complexité de Kolmogorov à ressources bornées. Ils montrent également dans [LP22a] que dérandomiser (cf. ci-dessous) revient à montrer que la complexité de Kolmogorov est difficile à approcher.

Dans la même veine, Hirahara [Hir18] montre comment dépasser, grâce à la méta-complexité, une barrière qui empêchait de ramener la complexité dans le pire cas à la complexité en moyenne (voir aussi [Hir22]). Ainsi, la méta-complexité permet en particulier de relier les bornes inférieures sur les circuits, la complexité de Kolmogorov et la dérandomisation, raison pour laquelle elle nous intéresse ici.

Dérandomisation L'autre versant consiste à étudier directement les bornes inférieures sur les circuits, ou la dérandomisation (suppression de l'aléatoire dans les algorithmes), deux questions centrales en complexité. Elles ont cette fois comme point d'intersection le problème PIT (Polynomial Identity Test) de décider si un circuit arithmétique calcule le polynôme nul. Il s'agit de l'un des rares problèmes naturels pour lesquels on connaît un algorithme probabiliste polynomial, mais pas d'algorithme déterministe efficace.

Nous disions que celui-ci est à l'intersection des bornes inférieures et de la dérandomisation pour la raison suivante. D'une part, une série d'articles (en particulier [Yao82 ; NW88 ; IW97]) montre comment déterminiser (*dérandomiser*) les algorithmes probabilistes, en particulier celui pour PIT, si certains problèmes n'ont pas de circuits de taille polynomiale. Puis, dans l'autre direction, Kabanets et Impagliazzo [KI03] montrent que dérandomiser PIT implique une borne inférieure non uniforme hybride, soit sur les circuits booléens soit sur les circuits arithmétiques. Ce résultat a encore été affiné récemment dans [AKT25]. C'est ce lien entre complexité booléenne, complexité arithmétique et dérandomisation qui nous intéresse ici.

Sujet de thèse

Bornes inférieures et dérandomisation Nous savons, grâce au résultat de Kabanets et Impagliazzo mentionné ci-dessus, que si $\mathsf{PIT} \in \mathsf{P}$ alors soit le permanent n'a pas de circuits arithmétiques de taille polynomiale, soit NEXP n'a pas de circuits booléens de taille polynomiale. Plutôt qu'une borne inférieure hybride entre circuits booléens et arithmétiques, nous pourrions vouloir une borne inférieure portant seulement sur les circuits arithmétiques. Il suffirait pour cela de définir une classe algébrique VNEXP qui contiendrait le permanent et qui, si elle avait des circuits arithmétiques de taille polynomiale, impliquerait $\mathsf{NEXP} \subset \mathsf{P/poly}$. Une première partie de la thèse consisterait à définir et étudier une telle classe, afin de comprendre les polynômes qu'elle contient. (Nous pourrions bien sûr vouloir obtenir des bornes inférieures booléennes pures via un théorème de transfert dans l'autre sens, mais cela semble inaccessible en début de thèse, cf. [KP11].)

Plus généralement, il s'agirait de comprendre plus en profondeur ce résultat de Kabanets et Impagliazzo et ses extensions récentes car celui-ci donne, sous l'hypothèse $\mathsf{PIT} \in \mathsf{P}$, une méthode pour montrer des bornes inférieures via des théorèmes de transfert entre le monde algébrique et le monde booléen. En particulier, en y regardant de plus près, l'hypothèse $\mathsf{PIT} \in \mathsf{P}$ est en réalité trop forte : il apparaît qu'il suffirait en fait de dérandomiser PIT seulement sur les polynômes multivariés de petit degré. C'est une piste qui devrait être explorée également, par exemple en évaluant le polynôme sur des entiers croissant suffisamment vite : la forme de l'entier ainsi obtenu est assez particulière pour espérer trouver un non-diviseur. En cas de succès, cela donnerait ainsi des bornes inférieures inconditionnelles.

Enfin, s'il semble raisonnable de tenter de dérandomiser cette version restreinte de PIT, la version générale semble quant à elle hors de portée. Plutôt qu'une dérandomisation, il s'agirait alors de montrer que ce problème ne peut tout de même pas être *trop difficile*, par exemple qu'il ne peut pas être EXP-complet. C'est une version allégée de la question $\mathsf{EXP} = \mathsf{RP}$ vers laquelle nous nous tournons maintenant grâce à la méta-complexité.

Méta-complexité Une des questions centrales dans ce domaine est de construire efficacement un mot ayant une grande complexité de Kolmogorov (on parle ici de complexité de Kolmogorov à ressources bornées car la version générale est indécidable). De nombreux articles traitent de la question, récents (par exemple [KK25 ; Hir+24]) ou moins récents (par exemple [Buh+05 ; Per07]). L'idée est de comprendre si la construction d'un tel mot est possible dans EXP sous l'hypothèse $\mathsf{EXP} = \mathsf{RP}$. En effet, si le mot construit est de complexité superpolynomiale, alors il ne peut pas être dans $\mathsf{P/poly}$, et on aurait donc

$$\mathsf{EXP} = \mathsf{RP} \implies \mathsf{EXP} \not\subset \mathsf{P/poly} \implies \mathsf{EXP} \neq \mathsf{RP},$$

ce qui séparerait EXP et RP.

Lors du stage de M2 de Micol, nous avons développé plusieurs outils pour cela, comme un test approché pour la complexité de Kolmogorov sous l'hypothèse $\mathsf{EXP} = \mathsf{RP}$ ainsi qu'une adaptation de la méthode d'extension de complexité de [Buh+05] à base de graphes expanseurs. Il s'agirait en thèse de poursuivre cette étude, en utilisant potentiellement d'autres mesures de complexité et ainsi d'autres outils de méta-complexité. Par exemple, la version restreinte mentionnée auparavant, à savoir montrer que PIT n'est pas EXP-complet, gagnerait sans doute à être approchée avec des adaptations algébriques des concepts généraux présentés ci-dessus pour la question $\mathsf{EXP} \neq \mathsf{RP}$.

Démarche scientifique

Comme pour tout travail de recherche, le sujet décrit ci-dessus évoluera évidemment en fonction des avancées de Micol d'une part, et des résultats de la communauté d'autre part. Nous pouvons néanmoins tenter l'exercice spéculatif d'établir un calendrier prévisionnel du début de thèse.

Les premiers mois seront bien sûr consacrés à l'appropriation des résultats existants en méta-complexité et dérandomisation (notamment sur PIT), en particuliers ceux mentionnés dans ce document. En parallèle, l'étude de la variante algébrique VNEXP de NEXP mentionnée ci-dessus est tout à fait accessible et pourrait donner lieu à des résultats rapides. À ce stade, et sans y rester bloqué trop longtemps, il nous semblerait légitime et intéressant d'étudier deux questions ouvertes liées :

— le calcul de grands entiers peut-il aider pour le permanent (dont les coefficients sont 0 et 1) ? Une réponse négative permettrait d'obtenir la conclusion générale du résultat de Kabanets et Impagliazzo en se contentant de la dérandomisation d'un version restreinte de PIT ;

— est-ce que $\mathsf{NEXP} \subset \mathsf{P/poly} \implies \mathsf{VP} = \mathsf{VNP}$, ou plus généralement quelle hypothèse booléenne plausible impliquerait que le permanent ait des circuits arithmétiques de taille polynomiale ? Une telle hypothèse pourrait permettre d'obtenir des bornes inférieures booléennes si $\mathsf{PIT} \in \mathsf{P}$.

En plus de ces deux questions, Micol pourrait commencer l'étude des questions $\mathsf{EXP} \neq \mathsf{RP}$ et surtout PIT non complet pour EXP, avec des idées nouvelles de méta-complexité et leur adaptation algébrique. Cette partie de la thèse devrait s'avérer très consistante et durer un certain temps pour nous amener au moins à la fin de la première année.

La suite de la thèse dépendra grandement des avancées de Micol et des collaborations qu'elle initiera. En particulier, nous comptons collaborer avec Rahul Santhanam (université d'Oxford), spécialiste reconnu de la méta-complexité et professeur invité au LIPN en mars, sur ces questions ainsi que d'autres en méta-complexité.

Références

[AKT25] Robert Andrews, Deepanshu Kush et Roei Tell. « Polynomial-Time PIT from (Almost) Necessary Assumptions ». *57th Annual Symposium on Theory of Computing, STOC 2025*. ACM, 2025, p. 1087-1095.

[Buh+05] Harry Buhrman, Lance Fortnow, Ilan Newman et Nikolai K. Vereshchagin. « Increasing Kolmogorov Complexity ». *22nd Annual Symposium on Theoretical Aspects of Computer Science, STACS 2005*. T. 3404. Lecture Notes in Computer Science. Springer, 2005, p. 412-421.

[Hir+24] Shuichi Hirahara, Valentine Kabanets, Zhenjian Lu et Igor C. Oliveira. « Exact Search-To-Decision Reductions for Time-Bounded Kolmogorov Complexity ». *39th Computational Complexity Conference, CCC 2024*. T. 300. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, 29:1-29:56.

[Hir18] Shuichi Hirahara. « Non-Black-Box Worst-Case to Average-Case Reductions within NP ». *59th Annual Symposium on Foundations of Computer Science, FOCS 2018*. IEEE Computer Society, 2018, p. 247-258.

[Hir22] Shuichi Hirahara. « Meta-Computational Average-Case Complexity: A New Paradigm Toward Excluding Heuristica ». *Bull. EATCS* 136 (2022).

[IW97] Russell Impagliazzo et Avi Wigderson. « *P = BPP* if *E* Requires Exponential Circuits: Derandomizing the XOR Lemma ». *29th Annual Symposium on the Theory of Computing, STOC 1997*. ACM, 1997, p. 220-229.

[KI03] Valentine KABANETS et Russell IMPAGLIAZZO. « Derandomizing polynomial identity tests means proving circuit lower bounds ». *35th Annual Symposium on Theory of Computing, STOC 2003*. ACM, 2003, p. 355-364.

[KK25] Valentine KABANETS et Antonina KOLOKOLOVA. « Chain Rules for Time-Bounded Kolmogorov Complexity ». *Electron. Colloquium Comput. Complex.* TR25-089 (2025).

[KP11] Pascal KOIRAN et Sylvain PERIFEL. « Interpolation in Valiant's Theory ». *Comput. Complex.* 20.1 (2011), p. 1-20.

[LP20] Yanyi LIU et Rafael PASS. « On One-way Functions and Kolmogorov Complexity ». *61st Annual Symposium on Foundations of Computer Science, FOCS 2020*. IEEE, 2020, p. 1243-1254.

[LP22a] Yanyi LIU et Rafael PASS. « Characterizing Derandomization Through Hardness of Levin-Kolmogorov Complexity ». *37th Computational Complexity Conference, CCC 2022*. T. 234. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 35:1-35:17.

[LP22b] Yanyi LIU et Rafael PASS. « On One-Way Functions from NP-Complete Problems ». *37th Computational Complexity Conference, CCC 2022*. T. 234. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 36:1-36:24.

[NW88] Noam NISAN et Avi WIGDERSON. « Hardness vs. Randomness ». *29th Annual Symposium on Foundations of Computer Science, FOCS 1988*. IEEE Computer Society, 1988, p. 2-11.

[Per07] Sylvain PERIFEL. « Symmetry of Information and Nonuniform Lower Bounds ». *Second International Symposium on Computer Science in Russia, CSR 2007*. T. 4649. Lecture Notes in Computer Science. Springer, 2007, p. 315-327.

[Yao82] Andrew Chi-Chih YAO. « Theory and Applications of Trapdoor Functions ». *23rd Annual Symposium on Foundations of Computer Science, FOCS 1982*. IEEE Computer Society, 1982, p. 80-91.