Le pseudo-aléa: objets et génération.

David Xiao
LIAFA
Université Paris Didérot - Paris 7
Case 7014
75205 Paris Cedex 13
dxiao@liafa.jussieu.fr

December 13, 2011

1 Introduction

1.1 Le pseudo-aléa et l'informatique

L'aléa est une ressource de calcul très importante. Il permet d'accelérer le calcul de certains algorithmes, comme le test de primalité des entiers, et il permet aussi de résoudre certains problèmes pour lesquels nous ne connaissons pas d'algorithme efficace et déterministe, comme pour le test d'identité des polynômes.

En général, on considère que l'aléa est une ressource chère. Les philosophes se doutent depuis toujours de l'existence de l'aléa; en tant qu'informaticien, on suppose que l'aléa existe, mais on veut l'économiser autant que possible. On veut aussi se munir d'outils pour utiliser de l'aléa défectueux, car même si l'aléa existe il peut être non-uniforme.

Nous verrons plusieurs méthodes pour économiser l'aléa. Nous verrons que grâce aux *graphes expandeurs*, on peut réduire l'erreur dans les algorithmes probabilistes sans aucun aléa supplémentaire. Nous verrons que les *extracteurs d'aléa* permettent de transformer une source d'aléa quelconque avec suffisament d'entropie en source d'aléa uniforme.

La possibilité d'économiser l'aléa nous mène à demander si l'aléa est nécéssaire dans ces algorithmes. Autrement dit, est-ce qu'il est possible de montrer que tout problème résolvable avec un algorithme probabiliste et efficace peut être résolu par un algorithme déterministe et efficace? Aujourd'hui, on sait que sous certaines conjectures la réponse est affirmative: sous ces conjectures, on peut construire des *générateurs pseudo-aléatoires* qui permettent de rendre déterministe (*i.e.* dérandomiser) tout algorithme probabiliste et efficace [NW94].

1.2 Le pseudo-aléa et les mathématiques

L'étude de l'aléa et de la probabilité dans les mathématiques remonte jusqu'au 17e siecle, mais l'idée du pseudo-aléa est assez récente. Le pseudo-aléa s'applique le plus souvent dans le cas où l'aléa est utilisé pour montrer l'existence de certains objets. Cette méthode, souvent appelée la *méthode probabiliste*, a été mise en valeur surtout par Erdős. En gros, la méthode probabiliste est le suivant: pour montrer qu'un objet avec une certaine propriété existe, nous définissons une

distribution de probabilité sur un univers adéquat et nous montrons qu'un objet tiré au hasard de cette distribution vérifie la propriété avec probabilité non-nulle.

De telles preuves d'existence ne donnent aucune indication comment construire de tels objets efficacement. Comme on a souvent besoin de constructions calculables en temps polynomial, il est donc nécessaire de refaire ces preuves pour qu'elles soient efficaces. Nous verrons l'exemple des codes correcteurs d'erreurs.

Finalement, nous regardons une autre application de l'idée du pseudo-aléa: le principe de transfert. Le principe de transfert dit en gros que si un ensemble est pseudo-aléatoire, alors ses sous-ensembles sont aussi pseudo-aléatoires. Il s'avère que ce principe s'applique aux nombres premiers, et il est l'un des ingrédients principaux de la démonstration du théorème de Green-Tao [GT08], qui dit que les nombres premiers contiennent des suites arithmétiques arbitrairement longues.

References

[GT08] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2):481–547, 2008.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. of Comp. and Sys. Sci.*, 49(2):149–167, 1994. Preliminary version in FOCS' 88.