

GENERIC CASE COMPLEXITY

organized by

Robert Gilman, Alexei Miasnikov, Vladimir Shpilrain, and Rebecca Wright

Workshop Summary

Introduction

This is a report by the organizers of the Workshop on Generic Case Complexity which took place at AIM the week of August 13-17, 2007.

Generic-case complexity is a new way to measure the difficulty of computational problems. It was originated by mathematicians for application to combinatorial group theory but seems well adapted to the important problem of estimating the algorithmic security of public key cryptosystems. So far the subject has been studied mostly by mathematicians. The organizers thought that the Workshop would afford an ideal opportunity to explore applications to cryptography.

Activities

The Workshop followed the prescribed AIM format. There were lectures in the morning, a two hour lunch period, and smaller group meetings in the afternoon. Refreshments were available throughout the day, and wine and beer were served at five o'clock. Keys were available for participants who desired to work outside the scheduled nine to five period. A banquet was held Tuesday evening.

As the topic of the workshop was new for some of the participants, it was decided in advance that the first few morning lectures would provide an introduction. Morning schedules for the remainder of the week were left open. Each afternoon lectures for the following morning were arranged following discussion with participants about what they would to hear. This system worked well.

During the afternoon members of the workshop divided into three or four groups to work on various problems. There was always one tutorial group for people who wanted more practise with the topics covered in the morning lectures. Other groups focused on various topics. One focused on applications of generic complexity to group theory and another another on applications to formal language theory. The latter topic is a new one, and will be the object of future research by some of the workshop participants.

Another topic for future research in Alexey Myasnikov's reformulation of the definition one-way function, which he presented in one of the morning talks. Alexey defines the same class of functions as usual but in a different language, the language of generic case complexity. This new prespective evoked expression of interest among the cryptographers.

Plans

During the discussion Friday afternoon there was a lot of enthusiasm for continuing to maintain the AIM web page associated with the workshop. There were a number of specific proposals including a list of active researchers and specific topics of research.

Conclusion

The Workshop had two specific goals. First to assemble a group of cryptographers and mathematicians in order to explore the potential contribution of generic-case complexity to cryptography and propose directions for future research. Second to provide an opportunity for mathematicians and cryptographers interested in mathematical aspects of cryptography to learn about generic-case complexity. There were not as many cryptographers present as we thought there would be, but there were enough to allow an interplay between cryptographers and mathematicians. In particular there were one or two very valuable afternoon sessions in which mathematicians were exposed to the research expectations of cryptographers. As one mathematician said, “Now I know why my papers keep getting rejected.”

In retrospect we might have done a better job in getting cryptographers to attend. Nevertheless the workshop did achieve its goals. As a result of the workshop it seems likely that research in the field will be directed more towards the discovery and analysis of cryptoprimitives, i.e., the mathematical problems underlying cryptosystems, and less towards the developing cryptosystems themselves. It is hard to think of another venue in which this could have occurred.

Informal attendance checks by the organizers indicated that attendance was very good with a slight decline Friday afternoon. Also it should be noted that support by AIM staff was excellent.