Semantics and Syntax

A Legacy of Alan Turing

Scientific Report

Arnold Beckmann (Swansea) S. Barry Cooper (Leeds)
Benedikt Löwe (Amsterdam) Elvira Mayordomo (Zaragoza)
Nigel P. Smart (Bristol)

1 Basic theme and background information

Why was the programme organised on this particular topic? The programme *Semantics and Syntax* was one of the central activities of the *Alan Turing Year 2012* (ATY). The ATY was the world-wide celebration of the life and work of the exceptional scientist *Alan Mathison Turing* (1912–1954) with a particular focus on the places where Turing has worked during his life: Cambridge, Bletchley Park, and Manchester. The research programme *Semantics and Syntax* took place during the first six months of the ATY in Cambridge, included Turing's 100th birthday on 23 June 1912 at King's College, and combined the character of an intensive high-level research semester with outgoing activities as part of the centenary celebrations. The programme had xx visiting fellows, xx programme participants, and xx workshop participants, many of which were leaders of their respective fields.

Alan Turing's work was too broad for a coherent research programme, and so we focused on only some of the areas influenced by this remarkable scientists: logic, complexity theory and cryptography. This selection was motivated by a common phenomenon of a divide in these fields between aspects coming from logical considerations (called *Syntax* in the title of the programme) and those coming from structural, mathematical or algorithmic considerations (called *Semantics* in the title of the programme). As argued in the original proposal, these instances of the syntax-semantics divide are a major obstacle for progress in our fields, and the programme aimed at bridging this divide.

The perception of the syntax-semantics divide as a major obstacle is not restricted to (the theoretical part of) academia. When Mike Lynch, the CEO of the company *Autonomy*, heard about our programme, his immediate reaction was that the syntax-semantics divide is highly relevant for the everyday practical work at Autonomy and decided to fund the programme with an extra £ 20,000 pounds. This additional money gave us some additional flexibility in the coordination of the programme.

What were the outstanding problems in the field? Our programme aimed at bridging the disciplinary gap between syntax and semantics in all of the subfields involved, but also at bridging other types of communication gaps between schools or research communities in the field. For instance, in cryptography, major issues that were tackled were the divides between theoretical work and the applications by the industry and between protocol analysis based on formal methods, and that based on complexity theoretic arguments.

A particular area of emphasis was the connection between computability and computational complexity, with interesting advances derived from the combination of methods from both. Examples of this were there successful revisiting of very low resource-bounded randomness (normality), Martin-Löf randomness (K-triviality, relative complexity, etc) and effective dimension (applications to random fractals). In complexity, leading researchers from descriptive complexity (Vardi, Kolaitis, Schweikardt, Väänänen, Dawar), from bounded arithmetic (Buss, Krajíček, Pudlak, Thapen, Jerabek, Beckmann), and those who already bridged

the gap (Cook, Atserias, Kolokolova) were brought together by the programme. *Semantics and Syntax* ensured that the different communities obtained a deep insight into the main outstanding problems of the other fields. For instance, in finite model theory the major open problem is whether there is a logic capturing on all structures the complexity class P of polynomial time decidable languages; in bounded arithmetic the major open problem is to prove strong independence results that would separate its levels; in propositional proof complexity the major open problem is to prove strong lower bounds for expressive propositional proof systems.

The programme also reached out to issues linking logic to some research areas in the (digital) humanities: a research group on formal models of narrative (Block, Fisseni, Léon, Löwe, Sarikaya), and one on natural language proof checkers for mathematical proofs (Alama, Cramer, Fisseni, Koepke, Schwichtenberg, Seyfferth, Tanswell) met during the programme in Cambridge, including both visiting fellows and guests.

How was the programme organised? Due to the embedding of the programme in the ATY, there was a large number of workshops and events. Some of the workshops doubled as the major international events of the relevant sub-communities (e.g., CCR 2012 was one of the SAS workshops). The heart of the programme was the *SAS Seminar*, a series of 30-minute informal lectures in which the new fellows presented open problems they intended to work on to the rest of the visiting fellows. Many participants also engaged with the wider research community in Cambridge, including various departments of the University of Cambridge (the Computing Lab, the mathematics departments, the Philosophy Department), some of the Colleges, Microsoft Research and some other companies (e.g., Cryptomathic, a Danish SME with an office in Cambridge). The programme had two distinguished fellows: Professor Shafi Goldwasser as the *Rothschild Professor* and Professor Martin Davis as the *Microsoft Distinguished Visiting Fellow*.

Beyond the immediate activity at the INI, there was a number of other Cambridge events that were intertwined with the research activity at the INI and brought more researchers in contact with the fellows. The international conferences *EuroCrypt 2012* and *CiE 2012* brought several hundreds of the leading thinkers of our fields to Cambridge.

2 Structure

Structure of the programme: As mentioned, the heart of the programme was the *SAS Seminar* meeting on Tuesday and Thursday afternoon in weeks without workshops. All speakers at the SAS Seminar submitted their abstract to a collection that will be published as the *Acts of the SAS Seminar* in the series *Texts in Computing* (College Publications; see below). In the following, we give brief descriptions of the seven workshops organized as part of the programme (including some of the positive and negative remarks obtained from the evaluations of participants):

1. **The Mathematical Legacy of Alan Turing** (Organiser: Benedikt Löwe). The first day of the programme was one of the LMS-funded *Spitalfields Days* in order to explain the subject matter of the programme to the wider academic public, and to get Cambridge mathematicians and computer scientists interested in the programme. Hugh Woodin, George Barmpalias, Nigel Smart, and Anuj Dawar gave research introductions to their respective fields, and many researchers from Cambridge and vicinity came, including an editor of the journal *Nature* (Tanguy Chouard). A report on the Spitalfields Day is published on pp. 20-21 of the April 2012 issue of the LMS newsletter.

2. **Is Cryptographic Theory Practically Relevant?** (Organisers: Kenny Paterson, Nigel Smart). This workshop tried to bridge the divide between theoretical cryptography and cryptography as practiced in industry. The event was highly successful with around one hundred participants from around the globe. The talks ranged from talks about the challenges phased by the banking industry, to to car security (both car locks, and the security of the electronic control systems), through to smart metering systems in the energy supply market. A number of new research directions arose from the workshop, including collaboration between academics and Cryptomathic on a system for securing messaging between HSMs (Hardware Security Modules) used in various banking applications.

The workshop was indeed so successful that within a week of it finishing companies were donating money to host a follow up even in 2013. After initially offering this to the Newton Institute (for logistical reasons the Institute was unable to accommodate it), we have settled on organizing the next event in Silicon Valley (`https://crypto.stanford.edu/RealWorldCrypto/`). So far the follow up workshop has attracted $\$50,000$ of corporate funding, and this is growing.

We received feedback from 40 workshop participants of which 97.5 % judged the scientific content either excellent or good and all judged the organization excellent or good. Some of the participants' comments: "I never saw a workshop with a so diverse and rich programme"; "very good mix between practical example and theoretical consideration"; "the topic was a great lightning conductor for thought and debate on an issue not normally addressed and ignored, but very important for the future"

3. **Pattern Formation: The inspiration of Alan Turing** (A Satellite Meeting at St. John's College, Oxford; organisers: Bernold Fiedler, Benedikt Löwe, Philip Maini). As mentioned, some of the exciting research areas that Alan Turing had worked in were not included in the scope of the programme. In order to make a link to these areas, we offered a satellite workshop to the morphogenesis community in Oxford. The workshop at St. John's College was seen in the SAS tradition to bridging gaps: here, it was the gap between the theoretical work of the mathematical biologist and the laboratory work that confirms or refutes the predictions of the theoretical model. The participants of this conference were from mathematics, biology and chemistry and emphasized the importance of including both theoretical and empirical research in the future agenda of morphogenesis. A number of important research collaborations were started at the workshop. (The journal *In Silico Biology* was very interested in getting the proceedings of the workshop as a special issue, but for health reasons, the organizers of the workshop could not accept that offer.)

4. **Logical Approaches to Barriers in Complexity II** (Organisers: Arnold Beckmann, Anuj Dawar). This workshop brought together leading researchers from the communities working on logical descriptions of complexity, i.e., descriptive complexity, propositional proof complexity and bounded arithmetic. It especially focused on work that draws on methods from the different areas which appeal to the whole community. We had 11 speakers from descriptive complexity including one tutorial speaker, 13 speakers from bounded arithmetic / propositional proof complexity including one tutorial speaker, and 3 speakers who's topic related to all areas. Highlights included reports on cutting edge research going on in each field (like Krajicek, Schweikardt), but in particular talks which clearly showed the impact of research of one community to research in the other (Atserias, Chen). We had many discussions after the talks and in particular during the breaks.

   We received feedback from 24 workshop participants who unanimously agreed that the scientific content and the organization were good or excellent (100% each). The workshop was very successful in stimulating more interaction between the two separate communities; one attendee, Professor Steven Lindell, stressed that he attended other meetings with a similar goal, but that this was the first time that it clicked between the communities. Professor Lindell's view was confirmed by many others.

5. **Formal and Computational Cryptographic Proofs** (Organisers: Nigel Smart, Shafi Goldwasser). This workshop aimed to bridge the gap between Formal Methods based approaches to verifying the security of cryptographic protocols and those based on complexity theory. For over a two decades the complexity theoretic approach has been considered the *de facto* standard way of performing such verification; with the approach via formal methods being considered almost fatally flawed. In recent years various researchers have found ways of repairing these flaws and the advent of automatic complexity theoretic verification of protocols via tools based on formal methods is becoming a reality.

   Highlights of this workshop included a number of talks on the world leading work in this area being performed by Microsoft Research in Cambridge, as well as work on automatic verification from researchers in France. A number of talks focused on the current hot topic of *fully homomorphic encryption*, with many of the main players in the field visiting the Newton Institute in this period. Different application

domains were considered, including the use of these techniques to verify the secure dismantling of nuclear weapons.

The workshop was attended by around 80 people, mainly due to it being followed by the EuroCrypt conference. A highlight of the conference was the Rothschild Lecture by Shafi Goldwasser on randomized algorithms.

We received feedback from 18 workshop participants who unanimously agreed that the scientific content and the organization were good or excellent (100% each). A comment from the evaluations: "This was the best event in crypto I have been to so far".

6. **The Incomputable** (A Satellite Meeting at Chicheley Hall, Newport Pagnell; organisers: Barry Cooper, Mariya Soskova). This workshop was bridging another gap: that between the mathematical theory of computability and its relevance for the real world. This is a core aspect of Turing's scientific legacy, and this meeting for the first time reunited (in)computability theory and 'big science' in a way not attempted since Turing's premature passing. The Incomputable had a stellar list of speakers including Samson Abramsky, Theodore Slaman, Yuri Matiyasevich, Sy Friedman, Julia Knight, Aaron Sloman, Christof Teuscher, Rodney Downey, Luciano Floridi, and Joel David Hamkins, and was generously supported by the John Templeton Foundation. The venue at Chicheley Hall made the event particularly attractive.

7. **7th Conference on Computability, Complexity and Randomness** (Organisers: Elvira Mayordomo, Wolfgang Merkle). This workshop constituted the 7th anual meeting of the active algorithmic randomness community. Its main added value is the joint of randomness researcher from both Computer Science and Mathematics. The meeting successfully included long discussion periods every afternoon as well as 31 specialized talks, including one on the applications of information theory to biology.

   We received feedback from 30 workshop participants who unanimously agreed that the scientific content and the organization were good or excellent (100% each). A comment from the evaluations: "The time for discussion every afternoon was very productive."

We should add some non-scientific concerns that were mentioned in the workshop evaluations by the participants: some workshop participants were not very happy with accommodation in Murray Edwards College and the food in Wolfson Court. Many people commented that the cafeteria food in the CMS or the lunch at Churchill College was far superior.

The formal dinner at Christ's College for the workshop *Logical Approaches to Barriers in Complexity II* was rated good. The dinner for the workshop *Formal and Computational Cryptographic Proofs* in April at Gonville & Caius was rated excellent. We had two dinners at Emmanuel College: the one in February for the workshop *Is Cryptographic Theory Practically Relevant?* was rated excellent to good, the one in July for CCR 2012 was rated excellent. Some of the participants regretted the fact that the historical locations of these formal dinners are not used for greater effect: historical introductions to the colleges and the architecture were missing.

3 Outcome and achievements

Scientific outcomes: It is far too early to describe the full extent of the outcomes of this very productive programme. Already now, only three months after the programme ended, there are over fifty preprints submitted to the INI preprint server. The main goal of the programme was to bridge a various divides, and the programme was certainly extremely successful in this, as is witnessed by the number of new collaborations triggered by the programme.

Collaborations: There is now a strong community growing which aims to bridge the divide between theoretical and industrial cryptography; as evidenced by the follow up workshop in Silicon Valley next year. In addition Bristol University is now collaborating with Cryptomathic on an authenticated encryption

method for use in HSMs in the financial sector. A lot of new interactions were forged with Microsoft Research in Cambridge, on various topics ranging from automated verification of protocols through to smart metering and zero-knowledge proof compilers.

The young algorithmic randomness community continued its expansion adding more contacts with Computer Science and even attracting a Biology researcher interested in the application of information theory to behavioral Biology.

In complexity theory, a focus point was the workshop *Logical Approaches to Barriers in Complexity II* which brought the two communities in logical description of complexity together. The workshop was very successful in stimulating more interaction between the two separate communities, with many participants confirming this view. In particular, new collaborations occurred between Beckmann, Pudlak and Thapen on connections between computational games and automatisability of proof systems; between Beckmann, Buss, Friedman and Thapen on set-theoretic analogues of time and space complexity classes (this collaboration was continued in September 2012, funded by an ESF Short Visit Grant); between Abramsky and Kolaitis on relations between quantum foundations and relational database theory.

Other new research connections involved the philosophy department of the University of Cambridge: in July 2012, the philosophy department organized a workshop entitled *Foundations of Mathematics* at Fitzwilliam College with a large number of Visiting Fellows of the programme *Semantics & Syntax* attending. A follow-up meeting entitled *History and Philosophy of Infinity* is planned in 2013 at Corpus Christi College.

How did the programme advance the state of understanding in the field? Major advances were being made in all field involved in the programme. In cryptography, new directions and tools were developed for the utilization of formal methods (syntactic) techniques to produce complexity theoretic (semantic) proofs. The combination of computability-theoretic and complexity-theoretic methods yielded a number of other breakthroughs such as the very efficient construction of absolutely normal numbers, and progress in Martin-Löf randomness (K-triviality, relative complexity, etc) and in effective dimension (applications to random fractals). Also in complexity theory, some connections with a potential for future research have been established, like the neat connection between the complexity of indistinguishability in counting logics and the complexity of proofs in certain semi-algebraic proof systems.

4 Publications

Books planned: As mentioned, we plan to publish the abstracts of the SAS Seminar and all of the workshops as a book entitled *Acts of the SAS Seminar* in the series *Texts in Computing* (College Publications). This book is complete and only requires some typesetting before it can be sent to the publisher.

Rod Downey and Mike Fellows have finished a book on parametrized complexity during the SAS programme.

Major papers or publications that were produced: As of 12 October 2012, the programme SAS has 51 preprints in the Newton Institute preprint series. We compared this to the number of preprints of the other INI programmes, and it is striking that only three months after the programme ended, the programme has the highest number of preprints submitted of all programmes at the INI since the preprint series started (second ranked is CPD (2003) with 44 preprints, and GMR (2005) and SPD (2010) are tied for third place with 43 preprints). Given the usual writing time of papers in our area, we expect that the number of preprints will grow significantly over the next year or so.

Video lectures: In our field, it is still rather unusual to have lectures videotaped and put online. The INI scheme of taping all lectures was something that our community had to experiment with. It seems that the idea was largely adopted by our field: according to the statistics on the Cambridge University server (21 October 2012), our top-viewed lecture was Nigel Smart's lecture at the Spitalfields Day (with 335 views), and there are five additional lectures with over 200 views, 18 more with over 100 views.

During the last week of June, there were over 1000 views of SAS-related videos in total; there were four further weeks (two in February, one in May and one in July) with over 500 views. These statistics match the ones of our sibling programme BSM (whose top video has 326 views, and they also have five more with over 200 views). Given that logic is a much smaller field than theoretical physics with far less general audience appeal, we consider matching the figures of BSM as a huge success of our programme.