Automated verification of complex systems in the energy sector

Smart energy grids and power networks are examples of complex systems that could benefit from quantitative analysis and certifiable policy synthesis grounded on formal computational models. Professor Alessandro Abate from the Department of Computer Science explains in this article how research is trying to validate innovative theoretical and computational techniques developed over complex models by tailoring them to real world applications, particularly in the energy sector.

Buildings consume more than 40 per cent of the total energy in Europe. It has been argued that efficient buildings automation systems can reduce their energy consumption by up to 30 per cent. In order to sustainably achieve this goal, reliable commissioning and maintenance of smart buildings automation systems is fundamental.

In an EU-funded project, my partners and I are seeking to show how developing automated verification and synthesis techniques over complex computational models could help achieve this goal. The 'Advanced Building Diagnosis and Maintenance' (AMBI) project is in collaboration with Honeywell Labs in Prague, Dresden University of Technology, and Delft University of Technology.

The project relies on a recently investigated mathematical framework called Stochastic Hybrid Systems (SHS) that is suitable for the quantitative description of devices and platforms where digital techniques are embedded in physical and analogue systems. SHS models are dynamical models that are able to characterise the probabilistic evolution of systems with interwoven and interacting continuous and discrete components.

SHS models can be used to quantitatively describe smart building systems, since they include physical quantities (such as temperature and humidity), as well as discrete elements (users' occupancy) and digital components (for example, ON/OFF taps or air conditioning modules expressible as finite-state models). Further, probabilistic terms originate from the presence of thermal noise, as well as from uncertainty in the weather affecting thermal loads and the associated generation of renewables (via solar and wind power). Uncertainty also affects sensor measurements, which are used to get access to quantities of interest (temperature, humidity).

Within AMBI we are currently developing both mechanistic and data-driven complex models tailored to smart building systems, with the overall goal of providing innovative solutions in diagnostics, prognostics and enhanced performance towards smart, optimised energy management.

Models for power networks

Additional current applications in the energy area deal with the use of formal abstraction techniques (see the later part of this article for more detail about this notion) over SHS models. In particular, I am interested in the development of models for demand-side participation of thermostatically controlled loads (that is, energy sinks, the consumption of which can be controlled), where the goal is to provide formal aggregated models for large-scale populations of thermal loads towards a practically useful optimal control of the generated power. This work is conducted in part in collaboration with German and American partners.

Related to this problem is that of formal aggregation of populations of photovoltaic panels (a project in collaboration with RTE, France), which aims to reduce instabilities in the global dynamics of power and frequency over regional, as well as large-scale, power transportation networks.

A notable benefit of working at Oxford is the presence of internationally visible colleagues in Computer Science who share my interests in energy and power applications, as well as the adjacency to the Engineering Department with its strong research emphases on Control Engineering, Artificial Intelligence and Machine Learning, and its focus on the more applicative development of state-of-

continued on next page ▶

from previous page ▶

the-art research. Oxford is also home to the Environmental Change Institute, which has an international track record for research in climate, ecosystems and energy.

Cyber-Physical Systems

As well as applications in the energy sector, I am interested in fundamental research in the areas of formal verification and of systems and control theory. The development of quantitative models for complex dynamical systems and the consequent reliance on them is pervasive in technology and in the sciences, and has matured from being a supporting methodology to becoming the foundational cornerstone of various disciplines. Understanding complex systems by establishing trust and control on their models is a goal with relevant downstream applications.

More recently, this trend has extended towards challenging areas, where the development and application of digital techniques is embedded within physical and analogue systems, and where the aspects of communication, computation and control are fully interleaved. Devices and platforms endowed with these heterogeneous physical/software, analogue/digital, continuous/discrete components and a high level of complexity are known as Cyber-Physical Systems (CPS), and are identified as a key research area by numerous industrial stakeholders, as well as governmental agencies such as the European Commission and the US National Science Foundation. The examples in the energy sector mentioned above can also be profiled as instances of CPS.

Effective progress in advanced applications such as CPS requires leveraging highly complex models: the involved dynamical features of CPS have recently led to an increased interest in the mathematical framework of SHS (mentioned above), which is regarded as a natural platform to comprise the elaborate intricacy of real-world applications of interest in CPS. SHS is a class of models presently investigated within the Hybrid Systems community, a research theme that in the past 15 years has brought together the heterogeneous expertise and orthogonal perspectives of researchers from both Engineering (systems & control theory, communication sciences) and the Computer Sciences (formal verification, dependability and performance analysis).

As one can expect, a general modelling framework such as that of SHS raises issues concerning analysis and associated decision (controller synthesis) problems: relying on manual (analytical) approaches towards analysis is ingenuous at best, whereas algorithmic procedures are bound to lack decidability or (optimistically) to tolling computational overhead. Simply put, formally proving theorems on SHS is hard, whereas computing over SHS models likely leads to state-space explosion problems (also known as the 'curse of dimensionality'). Yet we can mitigate these limitations by using new analytical approaches, as well as techniques for abstraction and compositionality, respectively.

Synthesis of formal abstractions

The main objective of this research line is to obtain formal model abstractions (i.e. simplifications that are mathematically related to the concrete, original models), with an explicitly quantified and adjustable approximation error. Such formal abstractions should be automatically employed towards synthesis and verification goals by leveraging modern, state-of-the-art software. In particular, 'finite abstractions' play a key role in dealing with problems that are structurally not decidable over models endowed with an uncountable (and in particular hybrid) state space and with continuous, probabilistic dynamics.

Finite abstractions can accommodate automatic model checking procedures and strategy synthesis algorithms, as implemented in existing software tools (e.g. SPIN, nuSMV, PRISM) that are having an impact in the academic and industrial context alike. It is in particular these new finite abstractions techniques that are used in the energy studies mentioned above.

The automatic synthesis of formal finite abstractions can be often aided and improved by proper a priori analysis of the model structure, which naturally leads to exploiting a modeller's expertise and deductive ingenuity. As an example, the tolling state space explosion problem mentioned above can be mitigated by employing tailored compositional approaches, or by developing results that are specification-dependent or driven by automatically synthesised counter-examples.

Overall, computationally the initiative aims at attaining fast algorithmic procedures that can scale acceptably with the model size, and it generally targets the development and testing of new dedicated software, as well as the integration of the proposed schemes with existing probabilistic verification tools.

An important benefit of working in the Department of Computer Science at Oxford is being able to take advantage of the excellent research environment in the automated and formal verification area, thanks to its emphasis on theoretical work and because of a number of state-of-the-art software tools being developed by colleagues.

In order to provide a clear experimental validation to the developed theoretical and computational techniques, I am engaged in applicative research that, as well as the energy domain, also spans the life sciences. In both areas I collaborate with experts in the specific domains, in order to achieve results that are compelling towards practical advancements, and which only collaborative research can truly foster in modern Engineering and Science.

For information or queries, feel free to contact me at aabate@cs.ox.ac.uk

More on finite abstraction tools can be found at: http://sourceforge.net/projects/faust2/ and http://sourceforge.net/projects/verisimpl/