Seminário em Engenharia Matemática

Data:31/05/2017
Horário:12h00
Sala: H211

Verificação Formal de Software

David Pereira
DEI e CISTER/ISEP

Os sistemas computacionais estão a tornar-se cada vez mais complexos e, portanto, difíceis de desenhar e implementar. Embora nas últimas décadas se tenha adotado metodologias guiadas por modelos e usado técnicas de geração automática de código a partir dos modelos produzidos, não é na generalidade garantido que o software produzido esteja livres de erros, o que, em última instância, leva a que os erros sejam apenas detetados durante a operação do sistema. No caso dos sistemas de alta integridade (aviões, satélites, mercados financeiros, dispositivos hospitalares, etc.), tais erros podem levar a situações catastróficas, incluindo a perda de vidas humanas.

Atualmente, as principais técnicas usadas para tentar garantir que os requisitos são realmente implementados, são baseadas em testes e/ou processos de simulação exaustivos que tentam dar a maior cobertura ao sistema possível, mas que têm um custo muito elevado. Mesmo assim, tal não é suficiente, pois no melhor dos casos consegue-se mostrar a presença de erros de implementação e não a sua ausência, algo que só é conseguido se para tal for construída uma demonstração matemática, verificável, que garante de forma unânime a correção das propriedades em questão.

Numa primeira fase deste seminário vamos abordar a questão da verificação formal de software, ou seja, a área que estuda teorias, modelos, metodologias e ferramentas com base matemática e que, portanto, permitem a possibilidade de produzir demonstrações da correção de resultados. Se o tempo o permitir, numa segunda fase vamos tentar ver na prática como construir demonstrações de propriedades de correção funcional usando o assistente de demonstrações Coq e observar quais os desafios que a utilização deste sistema (e similares) levantam, nomeadamente, no contexto empresarial.