Sumário

Asserções baseadas no conhecimento da aplicação podem ser especialmente eficazes na detecção de erros, originados por falhas de hardware ou software, que outros mecanismos independentes da semântica da aplicação não são capazes de detectar. Em particular, asserções com elevada capacidade de detecção de erros constituem uma área de investigação com muito interesse por proporcionarem uma cobertura de erros quase completa à custa de um baixo nível de redundância.

Começando por caracterizar os mecanismos de detecção de erros baseados em asserções de qualquer tipo, foram identificados como principais problemas desta abordagem a ausência de protecção dos dados fora do âmbito de cobertura das asserções e a necessidade de proteger a execução das próprias asserções.

Para solucionar estes problemas foi proposta a técnica de asserções robustas que permite obter, com um elevado grau de confiança, a garantia de que os resultados de uma computação foram filtrados por uma asserção correctamente executada, e que esses resultados não foram corrompidos após terem sido verificados. Saberemos nesse caso que os resultados, mesmo se errados, satisfazem o invariante definido pela asserção.

Dizemos que um tal sistema segue um novo modelo de avarias designado por avaria limitada. Este modelo, cuja aplicabilidade a qualquer sistema em que o programador possa definir asserções sobre o resultado foi demonstrada por injecção de falhas numa aplicação de controlo real, permite descrever o comportamento de muitos sistemas com baixa redundância de hardware e software.

Seguidamente são investigadas duas técnicas baseadas em asserções com elevada capacidade de detecção de erros, tolerância a falhas baseada nos algoritmos (ABFT[1]) e verificação do resultado (RC[2]), aplicáveis à maioria das operações sobre matrizes que constituem a base do cálculo científico.

ABFT é o nome dado a um conjunto de técnicas usadas para determinar a correcção do cálculo de algumas funções matemáticas, e cuja ideia base é codificar os dados, executar o algoritmo sobre os dados codificados, e, no fim, verificar se a codificação foi preservada. RC é uma técnica em que os resultados de uma computação são verificados através de cálculos adicionais mais simples que, contrariamente ao ABFT, são independentes do algoritmo usado.

O estudo comparativo dos dois métodos mostrou que o RC é uma alternativa vantajosa ao ABFT para detecção de erros. Sendo a primeira vez que o RC é avaliado através da injecção de falhas, mostrou-se que apesar de os dois métodos terem equivalente capacidade de detecção de erros, o RC tem um menor custo adicional de tempo de execução e que tem a importante vantagem de poder ser aplicado a qualquer algoritmo que resolva o problema em causa.

Para comprovar o valor prático do RC, desenvolveu-se um novo verificador de resultado para o problema do cálculo de valores e vectores próprios. A avaliação deste mecanismo, implementado sobre rotinas da biblioteca de domínio público LAPACK e usando a técnica das asserções robustas, revela um custo adicional de menos de 2%, para matrizes de média e grande dimensão, e uma cobertura de erros superior a 99.7% com um grau de confiança de 99%.

Concluímos que asserções com elevada capacidade de detecção de erros permitem construir, a um baixo custo, aplicações de elevada fiabilidade.

Palavras chave:

Detecção de erros, tolerância a falhas baseada nos algoritmos (ABFT), ABFT robusto, asserções, asserções robustas, verificação do resultado (RC), injecção de falhas, modelo de avarias, avaria limitada,
operações com matrizes, cálculo de valores e vectores próprios.

[1] Do inglês: Algorithm Based Fault Tolerance.
[2] Do inglês: Result-Checking.

Paula Prata, Dep. de Informática da UBI