Generación de Código con Certificado Asociado

Ricardo Peña Marí

31/01/2008

Resumen

Se explica un enfoque concreto dentro de la línea de investigación "Proof Carrying Code" (código con certificado asociado) en la que se pretende producir programas que satisface ciertas propiedades útiles y a los que se adjunta una demostración matemática de dichas propiedades.

Nuestro proyecto ha desarrollado un lenguaje funcional, llamado Safe, cuyo compilador esta provisto de una serie de análisis estáticos que aproximan ciertas propiedades útiles. Los análisis incluyen inferencia de regiones, de comparticion de estructuras, de tipos seguros, de terminación, y de inferencia de espacio.

La propiedades que garantiza son: cota superior al consumo de memoria, terminación, y ausencia de punteros descolgados. El código objeto producido por el compilador es 'bytecode' de la máquina virtual de Java. El objetivo final es convertir esas propiedades inferidas en demostraciones que puedan ser comprobadas automáticamente por un asistente de demostraciones estándar tal como Isabelle. En la presentación se resumen los aspectos relevantes del lenguaje y de sus análisis y se explica el enfoque seguido para la obtención de certificados.