Trabajo Práctico
Verificación de Software

Licenciatura en Ciencias de la Computación
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario
Rosario – Argentina

Maximiliano Cristiá
2023

- El trabajo práctico (TP) es individual.
- Se debe entregar por correo electrónico (cristia@cifasis-conicet.gov.ar) a más tardar el día que se presenten a rendir IS 2.
- Antes de empezar a resolverlo cada alumno debe seleccionar o inventar un problema, me lo debe comunicar por correo electrónico (cristia@cifasis-conicet.gov.ar) y debe esperar mi respuesta para comenzar. La idea es que yo voy a determinar si el problema es razonable o no.

  El problema que elijan o inventen no tiene por qué ser ni grande ni complejo. La especificación Z tiene que tener al menos dos operaciones o dos invariantes de estado. Pueden elegir problemas de la práctica y de los exámenes finales pero yo voy a controlar que dos alumnos no estén resolviendo el mismo problema.
- Una vez establecido el problema el alumno deberá:
  1. Formalizar el problema en Z.

     > Antes de empezar a escribir la especificación Z tienen que leer el Apéndice A del manual de FASTEST (ver más abajo) para conocer las cosas de Z que no pueden usar en la especificación porque FASTEST no las soporta.

  2. Traducir la especificación Z a un programa $\{log\}$ (setlog) que esté correctamente tipado (es decir se debe usar el *typechecker* de $\{log\}$).
     - $\{log\}$ es un lenguaje de programación de restricciones basado en Prolog.
     - Al traducir la especificación Z a $\{log\}$ se obtiene un prototipo (básicamente un programa escrito en el lenguaje de programación de $\{log\}$).
     - Para ejecutar $\{log\}$ necesitan instalar SWI-Prolog 8.4.2 o superior (SWI-Prolog es un intérprete de Prolog): http://www.swi-prolog.org/.
     - El sitio oficial de $\{log\}$ es este: https://www.clpset.unipr.it/setlog.Home.html.
     - Apunte de clase para aprender a traducir de Z a $\{log\}$: https://www.fceia.unr.edu.ar/ingsoft/tp/setlog.pdf.
     - Presentación (en inglés) sobre $\{log\}$: https://www.fceia.unr.edu.ar/ingsoft/tp/abz.pdf.

- Manual de usuario (en inglés) de $\{log\}$: https://www.clpset.unipr.it/SETLOG/setlog-man.pdf.

3. Ejecutar dos simulaciones no triviales sobre el prototipo. La ejecución de simulaciones sobre $\{log\}$ está explicada en el apunte de clase.
4. Usar el VCG para generar las condiciones de verificación. El VCG está explicado en el apunte de clase.
5. Descargar todas las condiciones de verificación generadas por el VCG. Esto también está explicado en el apunte de clase.
6. Demostrar con Z/EVES un lema de invariancia sin usar el comando `prove by reduce`.
7. Generar casos de prueba a partir de la especificación Z para una operación usando FASTEST y aplicando al menos dos tácticas de testing.
   - FASTEST es una herramienta desarrollada en el DCC que genera casos de prueba automáticamente.
   - FASTEST está acá: www.fceia.unr.edu.ar/~mcristia/fastest-1.7.zip. Necesitan tener instalado Java. En principio ejecuta sobre Linux y Windows. La distribución incluye un manual de usuario pero hacia el final de la materia vamos a explicar FASTEST y la teoría de testing que implementa.

   > Lamentablemente Z/EVES y FASTEST usan verisiones diferentes del lenguaje Z. Sin embargo, la única diferencia importante es que en Z/EVES se usa $\triangleq$ para definir esquemas (e.g. $A \triangleq A \vee B$) mientras que FASTEST usa $==$ (e.g. $A == A \vee B$). Esto significa que van a tener que tener dos archivos con la especificación.

- El TP se entregará en un archivo `.zip` o `.tar.gz` que deberá contener lo siguiente.
  - Un archivo `.tex` con el contenido del TP (ver más abajo).
  - El `.pdf` correspondiente.
  - El archivo con el código fuente del prototipo $\{log\}$ generado desde la especificación Z.
  - El archivo generado por el VCG.
- El contenido del TP es el siguiente.
  1. El problema inventado o elegido.
  2. La especificación Z incluyendo las designaciones que correspondan, más breves comentarios informales que expliquen la especificación.
  3. Las dos simulaciones ejecutadas sobre $\{log\}$ y la primera solución de cada una de ellas. El código de las simulaciones tiene que estar dentro de uno o dos entornos LaTeX del tipo `verbatim` y tiene que ser solo texto.
  4. Explicar cómo fue la interacción con el VCG: ¿Tuvieron que agregar hipótesis? ¿Usaron el comando `findh`?
  5. El enunciado del teorema que se probó con Z/EVES más los comandos de prueba que se usaron durante la demostración. El enunciado del teorema debe estar dentro de un entorno LaTeX del tipo `theorem` y los comandos de prueba dentro de uno del tipo `zproof`.
  6. Los comandos FASTEST que se usaron para generar los casos de prueba. Los comandos tienen que estar dentro de un entorno LaTeX del tipo `verbatim` y tiene que ser solo texto.

7. Los esquemas Z que corresponden a los casos de prueba generados.
8. Si FASTEST no genera un caso de prueba para alguna de las hojas del árbol de pruebas, se debe explicar el motivo.

En todos los casos se debe explicar qué es lo que se hace. Por ejemplo, se debe explicar coloquialmente las simulaciones, las pruebas, etc.

- Yo voy a corregir cada TP. Una de las cosas que voy a tener en cuenta es cómo está organizado, presentado y redactado el documento final (además, obviamente, de las cuestiones técnicas).

  Si los aspectos técnicos están bien pero la organización, presentación o redacción del documento final (incluye, por caso, la ortografía) no me satisfacen van a tener que mejorarlo. **Esto lo van a poder hacer solo una vez, caso contrario deberán volver a rendir IS 2 (todo, final y TP).**
  Claramente si los aspectos técnicos están mal, el TP y el examen quedan desaprobados y los deberán hacer nuevamente.

- Observen que pueden empezar a hacer el TP desde el primer cuatrimestre: NO TIENEN QUE ESPERAR A DOS DÍAS ANTES DE RENDIR IS 2. Apenas aprenden Z ya pueden seleccionar el problema, hacer la especificación Z, traducirla a $\{log\}$ y correr las simulaciones; al final del primer cuatrimestre pueden hacer las demostraciones con $\{log\}$ y Z/EVES. Al final del segundo cuatrimestre pueden hacer lo de FASTEST.