¿Cuál es el objetivo del trabajo?

El objetivo principal del trabajo es presentar la definición matemática de los RNGs y plantear cuales son los principios y criterios de calidad de un buen generador. En la sección 2, plantea cuales son las familias de generadores RNGs más conocidas y en la sección 3 propone un plan de pruebas, muy simple, con el cual en la sección 4 procede a evaluar algunos generadores de herramientas comunes y ver como fallan esa simple prueba.

Finalmente, en la sección 5, y como razón principal del trabajo enseña una herramienta de programación orientada a objetos, que cumple con los requisitos del autor para RNGs y muestra su potencial.

¿Qué generadores de números seudo-aleatorios discute? Teórico

Generators Based on Linear Recurrences

`xi = (a_1 * x_i-1 + ... + a_k * x_i-k) mod m`
Esto significa que la generación número i de un V.A. depende de la `k` generaciones anteriores. Dado un `m` primero y una ecuación correcta se puede llegar a un periodo de generación de tamaño `ρ = mk − 1`.

- K=1 linear congruential generator (LCG)
- K>1 multiple recursive generator (MRG)

Luego muestra otros generadores del mismo tipo pero que se calculan de distintas formas

- Linear feedback shift register (LFSR)
- Generalized feedback shift register (GFSR)

¿Qué generadores de números seudo-aleatorios discute? Práctico

Se plantean 2 test estadísticos que buscan probar 2 propiedades distintas de los RNG. El primero separa el dominio y se trata de observar la cantidad de colisiones que hay en los números generados. El segundo también separa el dominio pero en cierto orden y mide cual es la separación entre los números generados.

Se experimenta con los generadores de Java, VB, Excel, LCG16807, MRG32k3a y MT19937. Todos fallan al menos una de las pruebas realizadas.

¿Cuáles son los hallazgos de esta investigación, y cuáles las conclusiones y recomendaciones presentadas por el autor?

El primer claro hallazgo es que no se puede confiar en todas las herramientas disponibles para generar números aleatorios. Por otra parte dice que un estándar obligatorio es tener múltiples streams generadores de números aleatorios independientes entre sí. Por último, habla de la herramientas construida por él y otros programadores la cual es considera brinda las herramientas básicas (en cuanto a que un buen generador debe tenerlas).