고급 소프트웨어 실습

분반: 4분반

학번: 20191583

이름: 김태곤

과제 1. LCG, MT 이외의 난수 생성 방식에 관하여 3가지 이상 열거하고 설명하시오. (폰트 10, 반페이지 분량)

LCG, MT 이외의 난수 생성 방식에는 중앙 제곱법, XOR 시프트, 역 합동 생성기(ICG)가 있다.

중앙 제곱법이란 임의의 숫자를 제곱하여 나온 숫자의 일부분을 선택해 난수를 만드는 방법이다. 폰 노이만이 1949년에 고안한 의사난수법으로, 현재는 품질이 좋지 않아 잘 사용되지 않는다. 중앙 제곱법은 $[X_{n+1} = (X_n)^2$의 가운데 a자리]로 나타낸다. 예를 들어 대상값이 1234이면 제곱은 1522756이 되고, a=3인 경우를 구하면 227이 된다.

XOR 시프트 방식은 말 그대로 XOR과 SHIFT 연산을 사용하는 난수 생성법이다. 사용하는 비트의 수에 따라 $2^{n\,bits}-1$의 난수 반복 주기를 갖는다. MT와 원리는 비슷하나 구현이 훨씬 간단하고 작동이 빠르다. 다만 난수 품질 테스트에 통과하지 못했고, 이를 해결하기 위해 Xoroshiro 128+ 등 다양한 변종 알고리즘이 나오고 있다.

마지막으로 역 합동 생성기(ICG)는 비선형적인 유사 난수 생성기로, LCG의 연속된 난수가 가지고 있는 상관관계를 없애기 위해 합동 곱셈에 대한 역원을 사용하는 알고리즘이다. ICG의 점화식은 $X_{n+1} = (aX_n^{-1} + c) \bmod m$ 으로 LCG에 X_n항의 역원을 사용항 형태이다. m=Prime Num, 0<a,c<m, $0 < X_0 < m$을 만족해야 한다. ICG는 합동 곱셈에 대한 역원을 계산해야 하므로 LCG에 비하여 느리다는 단점이 있다.