고급 소프트웨어 실습

분반: 수요일 분반

학번: 20171665

이름: 이선호

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

LCG 와 MT 이외의 컴퓨터 난수 생성 방식에는 중앙제곱법, XOR Shift 그리고 진정한 난수 생성기(True Random Number Generator)가 존재한다.

폰 노이만에 의해 공식적으로 발표된 중앙제곱법은 임의의 수를 제곱한 결과에서 원하는 자릿수인 가운데 일부분을 뽑아 다시 제곱해 가면서 난수를 생성하는 방식이다. 처음에 어떠한 수를 제곱하는지에 따라 뒤에서 생성되는 난수의 결과가 다를 가능성이 높지만, 경우에 따라서 같은 수가 계속 반복될 수 있어서 효율적이지 못할 뿐만 아니라 가운데 뽑은 자릿수가 0 이 되면 더 이상 난수를 생성해 가지 못한다는 단점이 있다.

XOR Shift 는 XOR 연산과 bit-shift 연산을 사용하여 난수를 생성하는 방식이며, Linear Feedback Shift Register 를 응용한 방식을 사용하는 메르센 트위스트의 방법과 유사하다. LFSR 이란 몇 개의 간단한 메모리 주소를 고르고, 초기화된 입력을 register 에 올려놓는다. 이후 오른쪽으로 비트를 하나씩 밀면서 오른쪽 끝에서 나온 비트를 가지고 미리 골랐던 메모리 주소에 있는 값과 함께 순서대로 XOR 게이트를 통과시켜서 왼쪽에 새로운 bit 로 추가시키는 방법이다. XOR Shfit 는 상대적으로 MT 보다 연산 속도가 빠르고 LCG 보다 품질이 좋지만, 일부 품질 테스트를 통과하지 못하는 경우가 있다는 단점이 존재한다.

앞서 소개한 방식은 매우 긴 주기와 무작위성에 가까운 확률을 가지고 그럴 듯한 난수를 생성하는 방법이지만, 이를 극복하고자 하드웨어를 통해 자연계에서 발견 가능한 무작위성을 관찰하여 진정한 난수를 만드는 방법도 있다. 예를 들어, CPU 사용률, 온도 등 난수를 생성하고자 하는 컴퓨터의 하드웨어로 관찰 가능한 여러 데이터를 종합하여 예측이 불가능한 난수를 생성하는 것이다.