고급 소프트웨어 실습

분반: 4분반

학번: 20192133

이름: 김아영

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

1. XOR 시프트(XOR shift)

XOR Shift는 Linear Feedback Shift Registe을 기반으로 한 의사 난수 알고리즘이다. 메르센 트위스트와 원리는 비슷하지만 구현이 훨씬 간단하고 작동이 빠르기 때문에 자주 사용된다.

XOR 과 비트 연산을 사용하는 난수 생성법으로, 비트연산을 한 값에다가 XOR 연산을 수행하면 XOR Shift가 완성된다. 구조상 현대의 컴퓨터에서 연산 속도가 매우 빠르고 품질도 선형합동법보다 좋다. 하지만 긴 주기를 얻기 위해서는 알고리즘에 들어가는 값을 잘 설정해야 하며, 몇몇 난수 품질 테스트를 통과하지 못하는 경우가 있어 여러 변종이 나와 있다.

1. WELL

WELL은 MT의 디자이너가 10년후에 고안한 난수 생성 알고리즘이다. 메르센 트위스터를 개선한 알고리즘으로, mt 알고리즘보다 더욱 빠르다고 한다. 균등한 랜덤의 분포도를 가지며, 분포도에 따라 WELL512, WELL1024, WELL19937, WELL44497이 있다. 숫자가 클수록 분포도가 높다.

1. 중앙제곱법(Middle-square Method)

중앙제곱법은 폰 노이만이 1949년 고안한 의사 난수 생성법으로, 임의의 숫자를 제곱한 다음 이 숫자의 일부분을 택하여 새로운 난수를 만들어내는 방법이다. 위 수식에 따르면 시드(는 임의의 a 자리인 수이고 X는 난수 수열, a는 얻고자 하는 난수의 자릿수이다.

임의의 4자리 난수를 생성하고자 한다면 다음과 같은 과정으로 생성한다. 먼저 임의의 숫자를 초기 값으로 선택한다. 두번째로 숫자를 제곱하여 중앙 부분의 4자리 숫자를 택하여 난수로 선정한다. 이 과정을 반복하여 난수 수열 X를 얻는다.

하지만 이 방법은 유사난수법으로, 생성된 품질이 높지 않은 편이다.