고급소프트웨어실습I

1주차 보고서

20171646 박태윤

1. Linear Congruential generator(선형 합동 생성기)

C(C++)의 rand와 srand에서 쓰이는 알고리즘이다. 다음과 같은 점화식을 통해 난수를 생성한다.

(m > 0, 0 < a < m, 0 < c < m, 0 <= < m)

이 때, 선형 합동 생성기 알고리즘을 사용해서 난수를 생성하면 주기가 생기게 된다. 난수의 주기는 m의 나머지로 난수가 생성이 되기 때문에 아무리 커야 m이고, 실제로는 이 주기는 훨씬 짧은 경우가 많기 때문에 완벽한 난수 생성기라고 보기는 어렵다. 난수의 주기가 m이 되려면 다음의 3가지 조건을 만족시키면 된다.

- c와 m은 같은 수로 똑같이 나누어 지지 않는다.(c와 m이 서로소이다.)

- a-1이 m의 모든 소인수로 나누어진다.

- m이 4의 배수라면 a-1도 4의 배수이다.

rand와 srand에서는 seed를 개발자가 설정할 수 있는데, seed는 위의 점화식에서 에 해당한다고 볼 수 있다.

2. Mersenne Twister(메르센 트위스터)

난수 반복 주기가 메르센 소수인데서 유래했다. 메르센 수는 으로 나타내어 지는 수이며 메르센 소수는 이 수들 중에서 소수인 것을 말하는 것이다. C++에서는 mt19937로 메르센 트위스터 난수 생성기를 사용할 수 있는데, 19937의 의미는 난수의 반복 주기가 이라는 것이다. 알고리즘의 동작 원리는 다음과 같다.

1.seed number를 사용하여 624 만큼의 길이를 가진 벡터를 생성한다.

2.이 벡터를 통해 624개의 난수를 생성한다.

3.벡터에 노이즈를 준 뒤 다시 2번 반복하는데, 노이즈를 주는 행위를 트위스트 한다고 한다.

C의 표준 랜덤 함수의 경우 의 주기를 가지는데 반해, 메르센 트위스터는 그보다 훨씬 큰 의 주기를 가진다. 또한 추가적인 장점으로 메르센 트위스터 알고리즘은 비트 연산만으로 구현이 되어 있기 때문에 연산 속도 또한 표준 rand()보다 빠르다.