고급소프트웨어실습1 Week1 HW

- Linear congruential, Mersenne twister -

컴퓨터공학 20172141 김미소

1. Linear congruential 난수 생성 방법

선형 합동 생성기는 다음과 같이 정의된다.

$$X_{n+1} = (aX_n + c) \mod m$$

각 인자의 범위는 m > 0 and a < m, c < m, X_0 < m이다. 선형 합동 생성기를 통해 생성되는 난수는 현재 난수의 영향을 받는 재귀 관계를 갖는다. 선형 합동 생성기는 인자(a, c, m)와 초기값의 영향을 받는데 이 인자가 어떤 수인가에 따라 주기가 짧아질 수도 있고 길어질 수도 있다. 최대 주기를 갖기 위해서는 c와 m이 서로소이고, a-1이 m의 모든 소인수로 나뉘어 떨어지며, m이 4의 배수인 경우 a-1도 4의 배수여야 한다. 선형 합동 생성기를 통해 생성되는 난수는 이전 상태를 반영하므로 다음 난수를 어느정도 예측할 수 있고 난수들 사이에서 상관관계가 존재하기 때문에 monte carlo simulation에 적절하지 않은 난수 생성기이다.

2. 메르센 트위스터 난수 생성 방법

메르센 트위스터의 이름은 메르센 소수에서 유래되었고 보통 2^{19937}-1의 주기를 갖는 mt19937을 이용한다. 기존의 rand함수는 2^{32}의 반복주기를 가지므로 이에 비하면 굉장히 큰 반복 주기를 갖는 것이다. 알고리즘의 동작 원리는 하드웨어 노이즈나 오늘 날짜를 seed로 사용하여 길이가 624인 가진 벡터를 생성한다. 그리고 이 벡터를 사용하여 624개의 유사 난수를 만들고 다시 이 벡터에 노이즈를 주어(twist) 624개의 유사 난수를 만든다. 메르센 트위스터는 twist 과정에서 LFSR(Linear Feedback Shift Register)를 약간 변형한 GFSR(Generalized Feedback Shift Register)를 사용한다. 메모리 주소를 몇 개 골라 놓고 seed를 레지스터에 넣은 후 오른쪽으로 한 칸씩 비트가 shift한다. 오른쪽 끝에서 빠져나온 한개의 비트를 미리 골라 놓았던 메모리 주소값과 순서대로 하나씩 XOR 게이트에 통과시키면 다음 input을 얻을 수 있고 이 과정을 반복하는 것이다.