고급소프트웨어실습1

1주차 과제 보고서

20161663 허재성

선형 합동법(Linear congruential generator)는 다음과 같은 재귀 관계로 순열 X_i가 반환된다.

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

따라서 순열 X_i는 나눔수 m, 곱합수 a, 더함수 c, 초기값 X_0에 의해 결정된다. c와 m이 서로소이고 a-1이 m의 모든 소인수를 약수로 가질 때, m이 4의 배수일 때, a-1도 4의 배수일 경우 난수의 주기가 m으로 최대가 된다, 하지만 대부분의 경우 주기가 m보다 훨씬 짧아져서 질 좋은 난수를 생성할 수 없다. 컴퓨터에서 나눗셈 연산과 modulo 연산은 매우 느려서 난수 생성 속도도 빠르지 못하며 연속한 난수들 사이에 상관 관계가 커서 다음 난수를 예측이 가능하다. 따라서 몬테 카를로 시뮬레이션에 적절하지 않으며, 암호학적인 목적으로 사용하기에는 부적절하다.

후술할 메르센 트위스터 난수 생성기에 비하면 난수 생성 속도도, 생성한 난수의 질도 좋지 않지만 메르센 트위스터 난수 생성기에 비해 메모리 요구량이 적기 때문에 메르센 트위스터 난수 생성기를 사용할 수 없는 임베디드 환경에서 사용을 고려해볼 수 있다.

메르센 트위스터 난수 생성기(Mersenne Twister)는 1997년에 마츠모토 마코토와 니시무라 다쿠지가 개발한 유사 난수 생성기로 매우 질이 좋은 난수를 빠르게 생성할 수 있다. 이름은 난수의 반복 주기가 메르센 소수(2의 거듭제곱에서 1이 모자란 수 중 소수인 수, $M_n = 2^n-1$)인데에서 유래했다. 이 중 주기가 2^{19937}-1인 MT19937이 특히 많이 사용된다.

메르센 트위스터, 그 중에서 MT19937이 가지는 이점은 다음과 같다.

난수를 생성하는 주기가 2^{19937}-1로 실용적인 프로그램에서 사용하기엔 충분히 크며, 생성된 난수가 623차원까지 동일 분포되어 있다. 즉 난수 623개를 623차원 하이퍼큐브의 좌표에 점을 찍어도 일관성을 발견할 수 없어서 연속된 난수들의 연관성이 매우 낮으며 비트 연산만으로 알고리즘 구현이 가능하여 매우 빠른 속도로 난수를 구할 수 있다.

선형 합동법과 비교해서 메르센 트위스터의 단점은 생성기의 크기가 커서 임베디드 환경과 같이 매우 적은 메모리만 사용가능한 환경에서는 사용하기 힘들다. 또한 메르센 트위스터 알고리즘또한 암호학적으로 안전하게 설계된 알고리즘은 아니다.