1주차

고급소프트웨어실습I

담당교수: 박운상

분반: 4

학번/이름 : 20161565 권기윤

1. linear congruential 난수 생성 방법

Linear congruential generator(선형 합동 생성기)는 널리 알려진 유사난수 생성기이다. 해당 난수 생성기에서는 다음과 같이 정의된 수열 X를 반환한다.

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

선형 합동 생성기의 상태는 바로 이전에 생성된 난수이고, 이 난수는 최대 m가지 경우가 있다. 따라서 난수의 주기 또한 최대 m이다.

- 0 < m
- 0 < a < m
- $0 \leq c < m$
- $0 \leq X_0 < m$

따라서 선형 합동 생성기는 위와 같은 인자들에 의해 유일하게 결정된다. 대부분의 경우 이 주기는 훨씬 짧으며, 최대 주기를 갖기 위한 필요충분조건은

1. c 와 m이 서로소여야 한다.
2. a-1이 m의 모든 소인수로 나눠져야 한다.
3. m이 4의 배수일 경우, a-1도 4의 배수여야 한다.

이다.

선형 합동 생성기의 단점으로는

1. 인자들과 마지막으로 생성된 난수를 안다면 뒤에 만들어질 모든 난수를 예측할 수있다.
2. 생성해 내는 난수의 질이 그 인자에 따라 극적으로 달라지며, 인자에 따라서는 적절치 못한 초기값 때문에 문제가 생기기도 한다. (ex. c = X0 = 0)

출처

https://ko.wikipedia.org/wiki/%EC%84%A0%ED%98%95_%ED%95%A9%EB%8F%99_%EC%83%9D%EC%84%B1%EA%B8%B0

2. 메르센 트위스터 난수 생성 방법

메르센 트위스터는 TT800생성기의 개선판으로, 기존 생성기들의 문제점들을 피하면서 매우 질이 좋은 난수를 빠르게 생성할 수 있도록 설계되었다. 속도가 빠르고 난수의 품질이 높아 점점 많은 곳에서 채택되고 있으며, 흔히 주기가 $2^{19937}-1$인 MT19937을 사용한다.

메르센 트위스터의 특징으로는

1. 생성해내는 난수의 주기가 $2^{19937}-1$로 매우 크다.

2. 생성된 난수는 623차원까지 동일분포되어 있다. 즉, 난수를 623개까지 짝지어서 623차원 하이퍼큐브에 해당하는 좌표에 점을 찍어도 일관성을 발견할 수 없으며, 연속된 숫자들 사이의 관계가 매우 낮다.

3. 비트 연산만으로 알고리즘의 구현이 가능하기 때문에 매우 빠르다.

이 있다.

단점으로는

1. 생성기의 상태가 비교적 큰 편이라 매우 적은 메모리만을 사용할 수 있는 임베디드와 같은 환경에서는 문제가 된다.

2. 암호학적으로 안전하게 설계되어 있지않다.

가 있다.

출처

https://ko.wikipedia.org/wiki/%EB%A9%94%EB%A5%B4%EC%84%BC_%ED%8A%B8%EC%9C%84%EC%8A%A4%ED%84%B0