고급 소프트웨어 실습

분반: 1

학번: 20181683

이름: 전용본

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

1. 중앙 제곱법

중앙 제곱법은 폰 노이만이 1949년에 고안한 유사 난수 생성법으로, 임의의 숫자를 제곱한 다음 이 숫자의 일부분을 가져와서 새로운 난수로 만들어내는 방법이다.

|  |  |  |  |
| --- | --- | --- | --- |
| **페이즈** | **대상값** | **제곱값** | **난수** |
| 0 | 1234 | 1522756 | 1**5227**56 |
| 1 | 5227 | 27321529 | 27**3215**29 |
| 2 | 3215 | 10336225 | 10**3362**25 |

의 가운데 a자리, x는 난수 수열, a는 원하는 자릿수, seed()는 임의의 a자리 인 수

폰 노이만이 1949년에 고안한 의사난수법이다. 생성된 품질이 좋지 않기에 이 시대 이후에는 실습시간에 구현했던LCG를 주로 사용한다.

1. XOR 시프트

실습 시간에 사용한 난수 생성 알고리즘인 메르센 트위스트의 하위호환이라고 볼 수 있지만, 구현이 훨씬 간단하고 작동이 빠르기 때문에 사용되는 난수 생성 알고리즘이다. 몇몇 난수 품질 테스트를 통과하지 못하는 경우가 있어서 ANSIC 난수 생성 알고리즘으로는 채택되지 못했고 이를 해결한 방식이 존재한다. 의 주기를 가진다

uint64\_t s[2];

uint64\_t xorshift128plus(void) {

uint64\_t x = s[0]; uint64\_t const y = s[1]; s[0] = y; x ^= x << 23;

s[1] = x ^ y ^ (x >> 17) ^ (y >> 26); return s[1] + y; }

1. 양자난수생성기술

빛의 무작위성을 이용한 양자역학적 원리로 난수를 생성하는 기술이다. 특정 결정에 강한 레이저를 쪼였을 때 레이저 빛이 광자 쌍을 만들어내는 양자역학적 현상을 이용한다. 무작위로 0과 1의 bit을 생성하는 광자의 상태를 측정한 뒤 그 결과를 프로그램으로 난수를 생성하는 방식이다.

참조

1. [난수 발생기 성능 분석 보고서](https://repository.kisti.re.kr/bitstream/10580/7926/1/2007-090%20%EB%82%9C%EC%88%98%EB%B0%9C%EC%83%9D%EA%B8%B0%20%EC%84%B1%EB%8A%A5%EB%B6%84%EC%84%9D%20%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf)
2. [나무위키/난수생성](https://namu.wiki/w/%EB%82%9C%EC%88%98%EC%83%9D%EC%84%B1)
3. [[프리미엄 리포트] '갤럭시A 퀀텀'에 들어간 양자난수생성기란 어떤 장치인가](https://www.dongascience.com/news.php?idx=38581)