합동식의 병렬화 algorithm

Multicore system

합동식을 통한 병렬화

- 용어 정의
  - (a, b) mod (M)
    - a와 b는 법 M에 대해서 합동이다.
    - a와 b는 M으로 나눴을때 나머지가 같다.

- 특성
  - (a, b) mod(M) , (c, d) mod(M)이면 (ac, bd) mod(M) 이다.
    - 부분특성
      - (a,b) mod(M), (x, x) mod(M) 이면 (ax, bx) mod(M)이다.
      - (a, b) mod(M) 이면 (ax, bx) mod(M)이다.

점화식의 분석

- Random number 의 점화식
  - x(i+1) = ax(i) % M **or** (x(i+1),ax(i)) mod(M)
  - i = 1 일때
    - (x(2) , ax(1)) mod(M) → (ax(2), a^2 x(1)) mod(M)
    - (x(3) , ax(2)) mod(M) → (x(3), a^2 x(1)) mod(M) 이다.
    - ...
    - (x(n), ax(n-1)) mod(M)
      → (x(n), a^2 x(n-2)) mod(M)
      → (x(n), a^(n-1) x(1)) mod(M) 로 표현 가능.
  - 만약에 (a^(n-1), c) mod(M) 인 경우
    - (x(n), a^(n-1) x(1)) mod(M)
      → (x(n), cx(1)) mod(M) 으로 표현 가능
  - 즉 (a^(n-1), c) mod(M)에서 c의 값을 알고 있으면 x(n)의 값을 바로 찾을 수 있다.

x(n)을 찾는 방법

- (a, t(1)) mod(M)이라고 하자.
  - (a^2, at(1)) mod(M) == (a^2, t(1)^2) mod(M) 이다.
    즉 (a^2, t(2)) mod(M)일 경우 (t(1)^2, t(2)) mod(M) 이다.
  - (a^3, t(3)) mod (M) == (a^(2+1), t(1)t(2)) mod(M)이다.
    즉 (a^3, t(3)) mod(M)일 경우 (t(1)t(2), t(3)) mod(M)이다.

- (1), t(2), t(4), t(8), t(16)..... 과 같은 값을 미리 계산해두면
  - ex) x(100)번째 수는 어떻게 찾을까?
    - 100 = 64 + 32 + 4 로 표현 가능함.
    - (a^100, t(64)t(32)t(4)) mod(M) == (t(64)t(32)t(4), t(100)) mod(M)
    - (x(100), t(100)*SEED) mod(M) 을 통하여 x(100)을 바로 찾을 수 있다.

- 주의사항
  - overflow!!!!!!!!!!!!!!!.

- 추가 사항
  - Google 에 합동식 검색해보시면 추가적인 여러 합동식의 규칙들이 있습니다.
    이를 이용하면 더 빠른 알고리즘 구현도 가능합니다.