Toom-Cook

https://youtu.be/LUvfazypc5w

Toom-Cook

- 큰 정수에 대한 곱셈 연산을 수행하는 이유? **암호화**

- 문자열 암호화 방법
  - 문자열을 일련의 긴 정수로 변환
  - 암호화 키는 긴 정수 형태로 변환
  - 암복호화의 효율성을 위해 수백 자릿수(n)를 포함하는 긴 정수에 대한 산술 연산에 의존
    - 덧셈과 뺄셈의 경우, $O(n)$ 의 시간 소모
    - 곱셈의 경우, $O(n^2)$의 시간 소모 → 많은 숫자를 처리하기 때문에 비용↑

- 이와 같은 이유로 곱셈 실행시간에 대한 연구가 지속적
  - **관련 연구 : 카라츠바, Toom-Cook 알고리즘 등**

http://cs.indstate.edu/~syedugani/ToomCook.pdf

Toom-Cook

- 안드레이 **톰**과 스테픈 **쿡**이 제안한 **곱셈 알고리즘**
- 큰 정수인 a와 b를 곱하기 위해, 두 수의 길이가 l인 k 개의 작은 조각을 나눔
- k 가 커질수록, 곱셈의 내부 연산 복잡 $\rightarrow$ 전체 시간 복잡도 낮아짐.
- 각각의 나눠진 조각에 대해서도 다시 적용 가능
  - 조각이 작아질 때까지 재귀적 사용이 가능

https://en.wikipedia.org/wiki/Toom%E2%80%93Cook_multiplication

Toom-Cook

- 두 수의 작은 조각인 k **가 2인 경우 = 카라츠바 알고리즘**
  - 카라츠바 알고리즘은 ToomCook을 포함한 다른 곱셈 알고리즘의 디딤돌 역할
  - ToomCook은 실제로 각 숫자를 분할하여 여러 부분으로 곱하는 카라츠바 방법 기반
  - ToomCook은 카라츠바 알고리즘의 더 빠른 일반화 방법 → 더 복잡

- “Toom-3” 과 Toom-Cook”이라는 용어와 주로 혼용되어 사용됨

- Toom-3는 k = 3인 Toom-Cook 알고리즘을 의미
  - 정확한 표기 : ToomCook-3way
  - ToomCook-3way : 분할 횟수에 따라 곱셈 횟수 크게 감소

http://cs.indstate.edu/~syedugani/ToomCook.pdf

ToomCook-3way

- ToomCook - n way는 곱을 $2 * (\mathrm{n}) - 1$로 줄임 $(n = 3)$

- 연산을 진행할 피연산자를 동일한 길이(l) 의 3개로 분할

$$X(t) = x_2 t^2 + x_1 t + x_0$$

$$\mathrm{Y}(t) = y_2 t^2 + y_1 t + y_0$$

  - base $B = b^i$ 로 선택해주어야 함

$$i = max\lfloor \lfloor log_b m \rfloor / k \rfloor, \lfloor \lfloor log_b n \rfloor / k \rfloor + 1$$

ToomCook-3way 1단계 : 분할

- $b = 10^4$ 으로 가정, 한 자리에는 4개의 10진 정수가 들어감
- $B = b^2 = 10^8$

예)

- 1234567890123456789012 → 12 3456 7890 124 5678 9012

- 987654321987654321098 → 9 8765 4321 9876 5432 1098

$$P(x) = a2 * x^2 + a1 * x + a0$$

$$Q(x) = b2 * x^2 + b1 * x + b0$$

$$p(x) = m_2 x^2 + m_1 x + m_0 = 123456x^2 + 78901234x + 56789012$$
$$q(x) = n_2 x^2 + n_1 x + n_0 = 98765x^2 + 43219876x + 54321098$$

ToomCook-3way 2단계 : 평가

- $p(x)q(x) = r(x)$에 대한 연산을 하기 위해 아래의 연산 진행
  - 0,1,-1,-2, ∞ 을 x에 대입 (∞ 대신 최고차항인 2를 넣어 사용하기도 함)
- ∞ 은 최고차항을 의미하여 지금은 x^2을 의미

$$P(x) = a2 * x^2 + a1 * x + a0$$

$$Q(x) = b2 * x^2 + b1 * x + b0$$

$$\begin{aligned}
p(0) &= m_0 + m_1(0) + m_2(0)^2 = m_0 \\
p(1) &= m_0 + m_1(1) + m_2(1)^2 = m_0 + m_1 + m_2 \\
p(-1) &= m_0 + m_1(-1) + m_2(-1)^2 = m_0 - m_1 + m_2 \\
p(-2) &= m_0 + m_1(-2) + m_2(-2)^2 = m_0 - 2m_1 + 4m_2 \\
p(\infty) &= m_2
\end{aligned}$$

ToomCook-3way 2단계 : 평가

$$
\begin{aligned}
p(0) &= m_0 & &= 56789012 & &= 56789012 \\
p(1) &= m_0 + m_1 + m_2 & &= 56789012 + 78901234 + 123456 & &= 135813702 \\
p(-1) &= m_0 - m_1 + m_2 & &= 56789012 - 78901234 + 123456 & &= \boxed{-21988766} \\
p(-2) &= m_0 - 2m_1 + 4m_2 & &= 56789012 - 2\times78901234 + 4\times123456 & &= \boxed{-100519632} \\
p(\infty) &= m_2 & &= 123456 & &= 123456 \\
q(0) &= n_0 & &= 54321098 & &= 54321098 \\
q(1) &= n_0 + n_1 + n_2 & &= 54321098 + 43219876 + 98765 & &= 97639739 \\
q(-1) &= n_0 - n_1 + n_2 & &= 54321098 - 43219876 + 98765 & &= 11199987 \\
q(-2) &= n_0 - 2n_1 + 4n_2 & &= 54321098 - 2\times43219876 + 4\times98765 & &= \boxed{-31723594} \\
q(\infty) &= n_2 & &= 98765 & &= 98765.
\end{aligned}
$$

ToomCook-3way 3단계 : 점별곱셈

$$
\begin{aligned}
r(0) &= p(0)q(0) &&= 56789012 \times 54321098 &&= 3084841486175176 \\
r(1) &= p(1)q(1) &&= 135813702 \times 97639739 &&= 13260814415903778 \\
r(-1) &= p(-1)q(-1) &&= -21988766 \times 11199987 &&= -246273893346042 \\
r(-2) &= p(-2)q(-2) &&= -100519632 \times -31723594 &&= 3188843994597408 \\
r(\infty) &= p(\infty)q(\infty) &&= 123456 \times 98765 &&= 12193131840.
\end{aligned}
$$

ToomCook-3way 4단계 : 보간

- $r(x)$에 대한 미지계수 구하기 위한 과정

$$\begin{pmatrix} r(0) \\ r(1) \\ r(-1) \\ r(-2) \\ r(\infty) \end{pmatrix} = \begin{pmatrix} 0^0 & 0^1 & 0^2 & 0^3 & 0^4 \\ 1^0 & 1^1 & 1^2 & 1^3 & 1^4 \\ (-1)^0 & (-1)^1 & (-1)^2 & (-1)^3 & (-1)^4 \\ (-2)^0 & (-2)^1 & (-2)^2 & (-2)^3 & (-2)^4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix}.$$

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -2 & 4 & -8 & 16 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} r(0) \\ r(1) \\ r(-1) \\ r(-2) \\ r(\infty) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1/2 & 1/3 & -1 & 1/6 & -2 \\ -1 & 1/2 & 1/2 & 0 & -1 \\ -1/2 & 1/6 & 1/2 & -1/6 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r(0) \\ r(1) \\ r(-1) \\ r(-2) \\ r(\infty) \end{pmatrix}.$$

ToomCook-3way 4단계 : 보간

$r_0 \leftarrow r(0)$ $= 3084841486175176$

$r_4 \leftarrow r(\infty)$ $= 12193131840$

$r_3 \leftarrow (r(-2) - r(1))/3$ $= (3188843994597408 - 13260814415903778)/3$

$= \boxed{-3357323473768790}$

$r_1 \leftarrow (r(1) - r(-1))/2$ $= (13260814415903778 - (-246273893346042))/2$

$= 6753544154624910$

$r_2 \leftarrow r(-1) - r(0)$ $= -246273893346042 - 3084841486175176$

$= \boxed{-3331115379521218}$

$r_3 \leftarrow (r_2 - r_3)/2 + 2r(\infty)$ $= (-3331115379521218 - (-3357323473768790))/2 + 2\times12193131840$

$= \boxed{13128433387466}$

$r_2 \leftarrow r_2 + r_1 - r_4$ $= -3331115379521218 + 6753544154624910 - 12193131840$

$= \boxed{3422416581971852}$

$r_1 \leftarrow r_1 - r_3$ $= 6753544154624910 - 13128433387466$

$= 6740415721237444.$

$$\begin{aligned} r(x) = &\ 3084841486175176 \\ &+ 6740415721237444x \\ &+ \boxed{3422416581971852}x^2 \\ &+ \boxed{13128433387466}x^3 \\ &+ 12193131840x^4. \end{aligned}$$

ToomCook-3way 5단계 : 합성

$r(0)$					3084 8414	8617 5176
$r(1)$				6740 4157	2123 7444	
$r(-1)$			3422 4165	8197 1852		
$r(-2)$		13 1284	3338 7466			
$r(\infty)$	+ 121	9313 1840				
	121	9326 3124	6761 1632	4937 6009	5208 5858	8617 5176

ToomCook-4way

- ToomCook - 4 way는 곱을 $2 * (4) - 1$ 총 7개로 줄인 것
- $\boxed{0, 1, -1, 1/2, -1/2, 2, \infty}$의 값이 t값에 들어감

$$X(t) = x_3 t^3 + x_2 t^2 + x_1 t + x_0$$

$$Y(t) = y_3 t^3 + y_2 t^2 + y_1 t + y_0$$

각각에 대해 k=4일때, 계수값을 행렬으로 적음

k = 4

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 8 & 4 & 2 & 1 \\ 8 & -4 & 2 & -1 \\ 1 & 2 & 4 & 8 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} Z_{F_0} \\ Z_{F_1} \\ Z_{F_2} \\ Z_{F_3} \end{bmatrix} = M_4 \times F$$

각각에 대해 k=3일때, 계수값을 수식으로 적음

$$p(0) = m_0 + m_1(0) + m_2(0)^2 = m_0$$
$$p(1) = m_0 + m_1(1) + m_2(1)^2 = m_0 + m_1 + m_2$$
$$p(-1) = m_0 + m_1(-1) + m_2(-1)^2 = m_0 - m_1 + m_2$$
$$p(-2) = m_0 + m_1(-2) + m_2(-2)^2 = m_0 - 2m_1 + 4m_2$$
$$p(\infty) = m_2$$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 64 & -32 & 16 & -8 & 4 & -2 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} \times \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \\ C_6 \end{bmatrix} = M_7^{-1} \times C$$

보간 단계에 필요한 행렬

https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=3519&context=etd

Q & A