VE477 HW 8

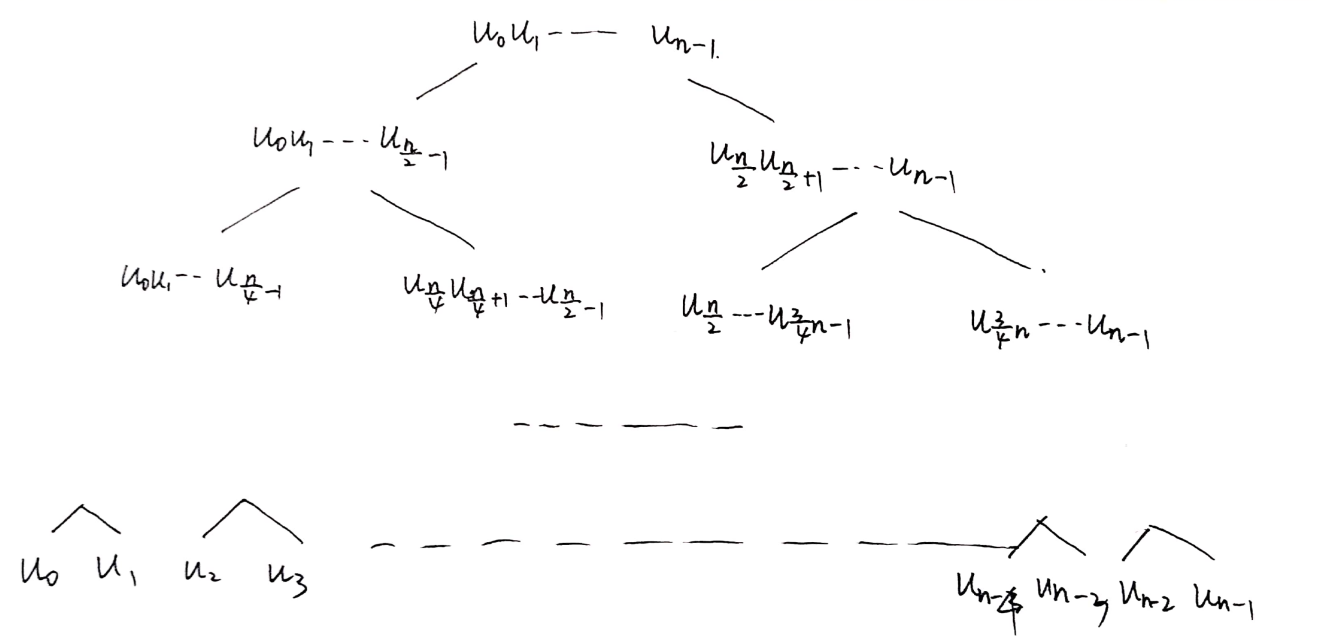
Wu Jiayao 517370910257

December 11, 2019

1 EX.1

Part I. Fast multi-point evaluation

1.1 Draw



1.2 Prove

$$
\begin{aligned}
M_{i+1,j} &= \prod_{l=0}^{2^{i+1}-1} m_{j\cdot 2^{i+1}+l} \\
&= \prod_{l=0}^{2^i-1} m_{j\cdot 2^{i+1}+l} \cdot \prod_{l=2^i}^{2^{i+1}-1} m_{j\cdot 2^{i+1}+l} \\
&= \prod_{l=0}^{2^i-1} m_{2j\cdot 2^i+l} \cdot \prod_{l=0}^{2^i-1} m_{2j\cdot 2^i+l+2^i} \\
&= \prod_{l=0}^{2^i-1} m_{2j\cdot 2^i+l} \cdot \prod_{l=0}^{2^i-1} m_{(2j+1)\cdot 2^i+l} \\
&= M_{i,2j} M_{i,2j+1}
\end{aligned}
$$

$$
M_{0,j} = \prod_{l=0}^{0} m_{j+0} = m_j
$$

1.3 Relate

The parent is the product of its two child. M_i, j has a depth $k - i$.

1.4 Evaluation

1.4.1 Subtree

Algorithm 1: Polynomial

Input : $X, k, \{u_0, u_1, \cdots, u_{n-1}\}$
Output: $M_{i,j}$

for $j = 0$ *to* $n - 1$ **do**
    $M_{0,j} = X - u_i$
for $i = 1$ *to* k **do**
    for $j = 0$ *to* $2^{k-i} - 1$ **do**
        $M_{i,j} = M_{i-1,2j} + M_{i-1,2j+1}$
return $M_{i,j}$

1.4.2

Algorithm 2: $Down(f, k, i, M)$

Input : P,$k, \{u_0, u_1, \cdots, u_{n-1}\}, M_{i,j}$
Output: $\{P(u_0), P(u_1), \cdots, P(u_{n-1})\}$

```
if i == 0 then
    return f
left ← f mod M_{k-1,2i}
right ← f mod M_{k-1,2i+1}
left_part ← Down(left, k − 1, 2i, M)
right_part ← Down(right, k − 1, 2i + 1, M)
return {left_part, right_part}
```

Algorithm 3: The algorithm

Input : P,$k, \{u_0, u_1, \cdots, u_{n-1}\}, M_{i,j}$
Output: $\{P(u_0), P(u_1), \cdots, P(u_{n-1})\}$

```
return Down(P, k, 0)
```

1.5 Complexity and Correctness

The time complexity for constructing the subtree is $\mathcal{O}(M(n)\log n)$. The complexity of evaluation is

$$T(n) = 2T(n/2) + O(M(n))$$

Hence, time complexity is $\mathcal{O}(M(n)\log n)$.

Fast Interpolation

1.6 Explain

Omitted

1.7 Prove

$m^{'} = \sum_{i=0}^{n-1}(X-u_i)^{'}\frac{m}{X-u_i} = \sum_{i=0}^{n-1}\frac{m}{X-u_i}$. All coefficients of $(X-u_i)$ will be zero in m', the only term remains is $1/s_i$

1.8 Algorithm

Algorithm 4: $Up(f, k, i, M)$

Input : P,$k, \{u_0, u_1, \cdots, u_{n-1}\}, M_{i,j}$
Output: $\{P(u_0), P(u_1), \cdots, P(u_{n-1})\}$

```
if i == 0 then
    return {P(u_0), P(u_1), ..., P(u_{n-1})}
left ← Up(left, k − 1, 2i, M)
right ← Up(right, k − 1, 2i + 1, M)
return left × M_{k,1} + right × M_{k,0}
```

Algorithm 5: The algorithm

Input : P,$k, \{u_0, u_1, \cdots, u_{n-1}\}, M_{i,j}$
Output: $\{P(u_0), P(u_1), \cdots, P(u_{n-1})\}$

```
return Up(P, k, 0)
```

1.9 Complexity and Correctness

The time complexity for constructing the subtree is $\mathcal{O}(M(n)\log n)$. The complexity of evaluation is

$$T(n) = 2T(n/2) + O(M(n))$$

Hence, time complexity is $\mathcal{O}(M(n)\log n)$.

1.10 Possibility

More space should be set to do this calculation. If the memory space is allowed, there is Possibility.

2 Critical Thinking

2.1 Prove

Omitted

2.2 ve477

Let the value given to S_1 is v_1, S_2 is v_2.

- "I'm not surprised, I knew you couldn't know!".
  Let S be a property of a number. A number n with property S means that $\forall x < y$ that $x + y = n$, at least one of x, y is not prime.
  v_1 should be smaller than 54, otherwise, if v_2 is exactly $53n$, S_2 can know the value. All the even number can be ignored since they can be expressed as the sum of two primes.
  For the left odd number, such numbers have property S.

  $$11, 17, 23, 27, 29, 35, 37, 41, 47, 51, 53$$

- "Uhm... so now I know..."
  $\forall x, y$ that $xy = v_2$, there exists exactly one x, y such that $x + y$ has property S.

- "So do I!"
  v_1 should not be in $2^n + p$ by 2 ways, where p is a prime. Otherwise, when S_2 is sure to get an answer, S_1 still needs more information, $v_1 = 2^{n_1} + p_1$ or $v_1 = 2^{n_2} + p_2$ The left number is

  $$17, 29, 41, 53$$

  For 17, $17 = 4 + 13$, only one possible solution.
  For 29, $29 = 2 + 27 = 4 + 25$, that have two posiible solutions, so they cannot know still.
  For 41, $41 = 4 + 37 = 10 + 31$, that also cannot know.
  For 53, $53 = 6 + 47 = 16 + 37$.
  still not know. Hence, the only is $4, 13$.

2.3 Ants

When they collide, actually nothing happens, they just continue their walking as ants since every ant is the same. The maxium time should be 1s.

3 IDEA