

## Hw4-problemC

3180106238 吴杰

首先要证明输出的第一个字符串一定是  $n$  个  $a$

这里需要证明两个事实:

1. 对任意  $n$ , 一定存在  $n$  个  $a$  和  $n$  长度的字符串  $str$ , 使得其基于上述算法所得的哈希值相同。

证明:

令  $str[i]$  表示  $str$  第  $i$  个字符

$hsh[1][j]=0$ , 对任意  $1 \leq j \leq n$  成立

对任意字符串

我们取  $mo[k]=gcd(str[1]-'a', str[2]-'a' \dots str[n]-'a')$

则有  $hsh[2][k]=0$  任意  $1 \leq k \leq n$  成立

对任意给定的  $mo[k]$

若  $0 < mo[k] \leq 25$ , 取  $str[i]=mo[k]+'a'$

若  $mo[k] > 25$

可以这样找:

Initial  $i \rightarrow 0, hsh[2][j] \rightarrow 0$

While not found

Do increase  $i$

If  $Hsh[2][j]*base+'z'-'a' < mo[j]$

Do  $Hsh[2][j]=Hsh[2][j]*base+str[i]-'a'$

Else

{Do  $str[i]=mo[j]+'a'-Hsh[2][j]*base$

Found

}

综上, 对任意字符串存在  $n$  个  $a$  和  $n$  长度的字符串  $str$ , 使得其基于上述算法所得的哈希值相同, 切对任意给定的  $mo$ , 能找到  $str$  满足题意。

证毕。

2. 若长度为  $n$  的字符全为  $a$  的字符串对给定的一组  $mo$  找不到对应的  $str$ , 则该长度的其他字符串均不符合题意

证明:

由 1 中搜索字符串的方法知,  $hsh[2][j]$  在  $length(str)$  次运算中都没有做取模操作, 不妨把  $str$  看作 26 进制的数, 则每一个长度为  $n$  的字符串的值都不同, 且由于没有取模操作, 则不存在不同的字符串的  $hsh$  值相同。

证毕

3. 证明输出的第一个字符串一定是  $n$  个  $a$

证明:

由 2 知若需满足题目条件, 则输出一定全是  $a$  的字符串, 由 1 知, 这样的字符串对任意给定的一组  $mo$  都存在。

证毕

## 题目分析:

由上述结论知,  $hsh[1][i]=0$ , 对任意  $1 \leq i \leq N$  成立, 我们需要找到字符串 **str2** 满足三个条件:

- $Length(str1)=Length(str2)$
- $Hsh[1][i]=Hsh[2][i]=0$ , 对任意  $1 \leq i \leq N$  成立
- 满足条件 1,2 的字符串且字典序最小

思路: 从长度为 1 的字符串开始寻找, 找到第一个满足上述条件 1, 2 的 **str2** 即为字典序最小的字符串。

## 算法描述:

记  $Hash(i)$  为对当前字符串关于  $mo[i]$  做题目所给的哈希映射得到的值。  
 $si$  为字符串第  $i$  个字符

**Pseudo code:**

```
Length->1
Str2->"b"
For i->1 to N
{
    If Hash[i]==0
    Do continue;
    Else
    Do search next str2 satisfy Hash[i]==0

    If length(str2)>length
    Do length=str2
}
For i->1 to length
    Printf('a')
Printf(str2)
```

## 难点:

搜索下一个满足  $Hash[i]==0$  的字符串

此处需要从  $i$  为 1 的情况开始

先暴力从字符串 **b** 开始找(按照字典序递增), 得到第一个满足  $Hash[1]==0$  的字符串 **str2**, 开始找第  $i$  个 ( $i=2,3,4, \dots$ ) 满足条件的字符串, 该字符串一定满足  $Hash[i-1]==0$ , 否则所找的前一个并不能满足条件。也就是说, 若  $Hash[i]=k$ , 则对每一个  $si*m$ , 使得  $mk \bmod mo[i]==0$ , 且  $m$  为满足前面式子的最小正整数, 再对 **si** 做处理即可得到下一字符串:

Pseudo code:

K→Hash[i],m→0

While  $m \cdot k \bmod mo[i] \neq 0$

Do m++

For i→1 to length(str2)

If  $(si - 'a') \cdot m > \text{base } s(i+1)$

Do  $s(i+1) += (si - 'a') \cdot m / \text{base} + 'a'$ ,  $si = (si - 'a') \cdot m \% \text{base} + 'a'$

Else

Do nothing

If  $s(\text{length}(\text{str2})+1) \neq \text{null}$

Do Length(str2)++