2.(a) if $x \neq y$, then $h_j(x) = h_j(y) \Rightarrow x \bmod p_j = y \bmod p_j$

$\Rightarrow |x-y| \bmod p_j = 0$ and we know $|x-y| \le 2^{\lg_2 U}$

and consider the prime factorization of $|x-y|$, if we write them down as $|x-y| = p_1 p_2 p_3 \cdots p_k$ the product of all primes, we will know $p_i \geq 2$ for all $i$ and therefore $2^k \le |x-y| \le 2^{\lg_2 U}$. so that $|x-y|$ has at most $\lg_2 U \to O(\lg U)$ prime divisors and therefore the probability of picking a bad $p_j$ from $\cancel{O(\frac{\lg m}{m})}$ $O(\frac{m}{\lg m})$ primes is at most $O(\lg u) / O(\frac{m}{\lg m}) = O(\frac{\lg U \lg m}{m})$ and thus $\Pr_{r_j}[h_j(x) = h_j(y)]$

$$\le O\left(\frac{\lg m \lg U}{m}\right)$$

2.(b)

and hash $A + P_j$, hash $B + P_j$, hash $C + P_j$

The new algorithm is simple. first we hash the elements in $A, B, C \subseteq \{0, 1, \ldots n^{100}\}$ to $\{0, 1, \ldots n^4\}$ then we use Prof X algorithm on the hashed $A, B, C$ to solve the 3sum problems.

Then the running time for this Algorithm is simple hash all the elements $O(n)$ + Prof X's 3sum $O(n^{1.99}) \Rightarrow O(n^{1.99})$

but the correctness (the error probability) needs analysis: I claim that

$\Pr[\text{error}] = \sum_{a,b,c} \Pr[a+b \neq c,\ h_j(a) + h_j(b) = h_j(c) \text{ or } h_j(a) + h_j(b) = h_j(c) + P_j]$

Scanned by CamScanner

since that when our Algorithm returns true but also false and notice that is impossible to have $a+b=c$, and $h_j(a)+h_j(b)\neq h_j(c)$ and $h_j(a)+h_j(b)\neq h_j(c)+P_j$ which is the case for return false but actually true. since

$$h_j(a)+h_j(b) = \text{or} \begin{cases} h_j(a+b)+P_j \\ h_j(a+b) \end{cases}$$

if $a+b=c$ then $h_j(a+b)=h(c)$ for sure.

So we split the formula to 2 parts.

$$Pr[\text{error}] = \sum_{a\cdot b\cdot c} Pr[a+b\neq c,\ h_j(a)+h_j(b)=h_j(c)] + Pr[a+b\neq c,\ h_j(a)+h_j(b)=h_j(c)+P_j]$$

we know each part ~~[illegible]~~ is smaller than $Pr[a+b\neq c,\ h_j(a+b)=h_j(c)]$

$$\text{So } Pr[\text{error}] = \sum_{a\cdot b\cdot c} 2\,Pr[a+b\neq c,\ h_j(a+b)=h_j(c)] \leq \sum_{a\cdot b\cdot c} 2\,O\left(\frac{\lg n^{100}\lg n^4}{n^4}\right)$$

$$\leq O(n^3)\cdot 2\cdot O\left(\frac{\lg^2 n}{n^4}\right) = O\left(\frac{\lg^2 n}{n}\right)$$

so $Pr[\text{error}] < O\left(\frac{\lg^2 n}{n}\right)$ which obvious smaller than $1/4$ when $n$ is large

So. our algorithm meets the requirement.

Scanned by CamScanner