October 28, 2022 10:50 AN Cond. Lower Bounds from 350M (Contd) Thm I (Patrason '10) Assuming the ASSUM Conj, no O(n<sup>3-8</sup>) time algim for Zero-Weight Triangle for weighted graphs Zero- Wf Triangle 01 D ZSUM APSP Convolution-350M Problem Given ard. --, an.1, bo, --, bn-1, Co, --, Cn-1, decide Jik st. ait blei = 9k. (i.e. ] i, j s.t. ait bj= citi) (((min,t)-Convol: > ) (one-seq vers: Bi, j, ait aj = aitj]. Convot350M -> 350M : easy map  $a_i \rightarrow (i, a_i) \rightarrow iM + a_i$ ((i,ai)+(j,aj)=(k,ak))(impair j  $m_{i}$  =  $k + a_{i} + a_{j} = a_{k}$ (impair j  $m_{i} + a_{j} = a_{i+j}$ ) (impair j  $m_{i} + a_{j} = k + a_{k}$ ) (impair j  $m_{i} + a_{j} = k + a_{k}$ ) Reduce 350m -> Convol-350m (for ints) (Patrascu'10 / Kopelountz-Pettie-Porat'16 / C.-He'20) almost idee - hashing with 11.13

idea hashing with  
the property 
$$h(a) + h(b) = h(a+b)$$
  
i.e. "almost" linear fri  
e.g. pick random prime  $p \in (R/2, R)$   
define  $h(x) = x \mod R$ .  
Obs (i)  $h(a+b) = h(a) + h(b)$   
or  $h(a) + h(b) - P$   
(ii) for any fixed  $a, a' \in (U)$  with  $a \neq a'$ ,  
 $Pr(h(a) = h(a')] \leq \tilde{O}(R)$ .  
Pf of(ii):  $Pr(a \equiv a' \mod P)$   
 $= Pr(P \text{ is a prime divisor of a-a'})$   
 $= \frac{\# prime divisors of a-a'}{\# primes \min divisor of a-a'}$   
ellog  $R \leq O((\log U) R/\log R) = \tilde{O}(R)$ .  
Car for fixed set S of n numbers & fixed 8,  
the bucked  $B_{A} = (a \in S: h(a) = R)$   
has expected size  $\tilde{O}(R)$ .  
To solve 350m for set S of n numbers:  
choose  $R = n$ .  
call bucket  $B_{A}$  good if its size is  $\tilde{O}(1)$ .

