$\Rightarrow \boxed{\tilde{O}(\sqrt{n}\, t)} \rightarrow \tilde{O}(t)$

Lemma 2 If $S \subseteq [u]$ & # elems used $\leq k$,
then $\tilde{O}(k^2 u)$ time.

Pf: By D & C. . .

Will compute

$C_S^{(j)}[i] =$ true iff $\exists$ subset S of j elems summing to i

$$\left.\begin{array}{l} \text{for all } i = 0, \ldots, ku \\ \phantom{\text{for all }} j = 0, \ldots k \end{array}\right\}$$

Solve problem for $L = S \cap (0, \frac{u}{2}]$ recursively
and $R = S \cap (\frac{u}{2}, u]$

Combine

$$C_S^{(j)}[i] = \bigvee_{i', j'} \left(C_L^{(j')}[i'] \wedge C_R^{(j-j')}[i-i'] \right)$$

2D Convolution $\rightarrow$ can be mapped to 1D
(map (i,j) to $3ik + j$ ...)

array size $O(ku \cdot k) = O(k^2 u)$

time for convol is $O(k^2 u \log (\cancel{k^2} u))$

$$T(n,u) = T\left(n_1, \frac{u}{2}\right) + T\left(n_2, \frac{u}{2}\right) + O(k^2 u \log u)$$

for some n_1, n_2 with $n_1 + n_2 = n$.

but u does not decrease for R !

extra idea - let $\hat{R} = \{a - \frac{u}{2} : a \in R\} \subseteq [0, \frac{u}{2}]$

$$C_R^{(j)}(i) = C_{\hat{R}}^{(j)}\left[i - j\frac{u}{2}\right]$$

$k^2u \longrightarrow k^2u$

$k^2\frac{u}{2} \quad k^2\frac{u}{2} \longrightarrow k^2u$

$k^2\frac{u}{4} \quad k^2\frac{u}{4} \quad k^2\frac{u}{4} \quad k^2\frac{u}{4} \longrightarrow k^2u$

$\vdots$

total time $\boxed{O(k^2 u \log^2 u)}$. $\square$

Bringmann's Rand Alg'm ('17): $\tilde{O}(t)$ time

Improved Lemma 2 If $S \subseteq [u]$ & # elems used $\le k$,

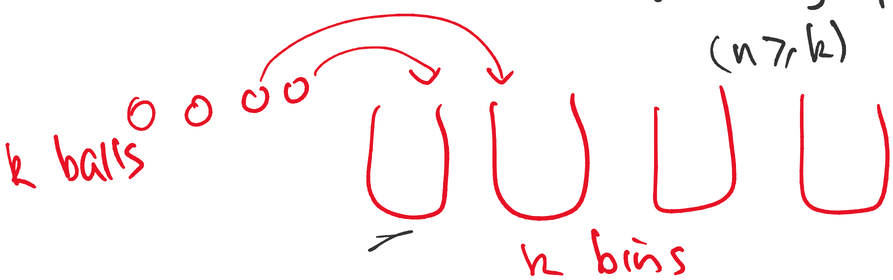
Improved Lemma 2 If $S \subseteq [u]$ & ...

then there is a rand algm with $\tilde{O}(ku)$ time.

Pf: idea - divide S into $\underline{S_1, \ldots, S_k}$ randomly

Fact Put k balls into k bins randomly.
Max # balls in any bin is $b = O(\log n)$ with high prob. $\geq 1 - \frac{1}{n}$.

$(n \geq k)$ $\left[O\left(\frac{\log n}{\log\log n}\right)\right]$



(Pf: Fix a bin.

$\Pr[\text{it has exactly } r \text{ balls}]$

$$= \binom{k}{r}\left(\frac{1}{k}\right)^r\left(1-\frac{1}{k}\right)^{k-r}$$

$$\leq \left(\frac{ek}{r}\right)^r\left(\frac{1}{k}\right)^r = \left(\frac{e}{r}\right)^r \leq \frac{1}{n^{10}}.$$

for $r \geq c\log n$ for suff large c.

$\Pr[\text{some bin has} \geq c\log n \text{ balls}]$

$$\leq n \cdot n \cdot \frac{1}{n^{10}}. \qquad \square\ ]$$

Given $S_1, \ldots, S_k$,

will compute

$C_{S_1 \ldots S_i}[i]$ = true iff $\exists$ subset with $\leq b$ elems chosen from S...

$C_{S_1,\ldots,S_k}[i]$ = true iff $\exists$ subset with $\leq b$ elems chosen from each of $S_1,\ldots,S_k$ summing to i

$(i = 0, \ldots, bku)$

Solve problem for $S_1, \ldots, S_{k/2}$ recursively & $S_{k/2+1}, \ldots, S_k$ recursively

Combine:

$$C_{S_1,\ldots,S_k}[i] = \bigvee_{i'} \left(C_{S_1,\ldots,S_{k/2}}[i'] \wedge C_{S_{k/2+1},\ldots,S_k}[i-i'] \right)$$

Convolution of two arrays of size $O(bku)$

$$T(k,u) = 2T\left(\frac{k}{2}, u\right) + O(bku \log u)$$

$$T(1,u) = \tilde{O}(b^2 u) \quad \text{by old Lem 2}$$

$$\Rightarrow \tilde{O}(bku \log^2 u)$$

$$\leq \tilde{O}(ku). \quad \square$$

$\Rightarrow$ Consider all $a_i \in (u/2, u]$

... $\tilde{O}(t)$ time

Try $u = 1, 2, 4, \ldots$

$\Rightarrow$ $\boxed{\tilde{O}(t)}$ total time

Jin-Wu's Alg'm ('19): Sketch

idea: polynomials

Suffice to compute

$$\prod_{a \in S} (1 + x^a) \mod x^{t+1}$$

& check coeff of x^t

e.g. $\{2, 5, 7\}$ $\quad (1+x^2)(1+x^3)(1+x^7)$

$= 1 + x^2 + x^3 + x^5 + \ldots$

How? $\exp\left(\sum_{a \in S} \ln(1+x^a) \right) \mod x^{t+1}$

use formal power series

$$\ln(1+x^a) = \sum_{i=1}^{\cancel{\infty}\ \lceil t/a \rceil} (-1)^i \frac{x^{ai}}{i} \mod x^{t+1}$$

& $O\left(\frac{t}{a}\right)$ time

total $O\left(t \underbrace{\sum_{a \le t} \frac{1}{a}}_{\text{Harmonic}} \right)$

$\sum_{i=1}^{t} \frac{1}{i}$

$= O(t \log t)$

Polynomial exponentiation reducible to poly mult. i.e. convol.

but needs to work in finite field $\mathbb{Z}_p$ for random p.

$\Rightarrow \boxed{O(t \log^2 t)}$ rand.