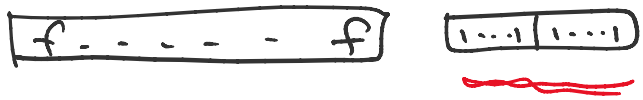
3. Set $t =$ 

use base $\max(f+1, 2^k)$

unfortunately, numbers too big

$t = 2^{O(m+n)} = 2^{O(n)} >> 2^n$.

next idea - reduce # vars & # constraints

divide into $\frac{n}{B}$ groups of B vars → "super-vars"

& $\frac{m}{B}$ groups of B clauses → "super-constraints"

each super-var lies in $[2^B]$

- each super-constraint contains $\leq kB$ supervars
- each supervar appears $\leq fB$ super-constraints

Lemma (from additive combinatorics, Behrend '46)

For any $N, M, \varepsilon > 0$, $\exists$ set of N numbers $\ell(1), \ldots, \ell(N)$ in $[M^{O(1/\varepsilon)} N^{1+\varepsilon}]$ which is M-average-free

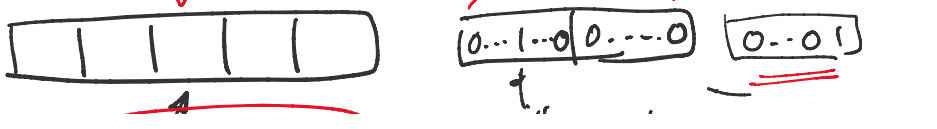
naively, M^N

i.e. $\frac{\ell(i_1) + \ldots + \ell(i_{M'})}{M'} = \ell(i)$, $M' \leq M$

$\Rightarrow \ell(i_1) = \ldots = \ell(i_{M'}) = \ell(i)$.

---

1. For each superconstraint C_j & each assignment φ of its $\leq kB$ supervars that satisfies C_j,

Create number $z(C_j, \varphi) =$ 

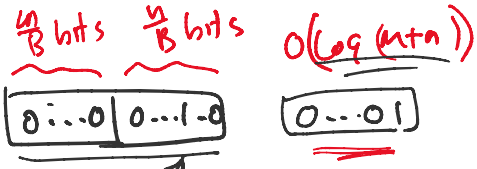
$z(C_j, \varphi) =$ 

i^{th} block is $\ell(\alpha_i)$ if Supervar $x_i = \alpha_i$ in φ
0 if supervar x_i is not in C_j.

j^{th} bit is 1
0 else

2. For each super-var x_i & each $\alpha \in [2^B]$, create number

$z(x_i, \alpha) =$ 



i^{th} block is $R - \text{freq}(x_i) \cdot \ell(\alpha)$
all other 0.

i^{th} bit is 1
0 else

3. Set

$t =$ 

where $\ell(\cdot)$ is from Lemma with $N = 2^B$,

$M = fB$,

$R = M \cdot M^{O(1/\varepsilon)} \cdot N^{1+\varepsilon}$

Correctness: let $f_i = \text{freq}(x_i) \le fB$

if we set $x_i = \alpha_1$ in C_1
$= \alpha_2$ in C_2,
⋮
then i^{th} column will sum to

$$\ell(\alpha_1) + \ell(\alpha_2) + \ldots + \ell(\alpha_{f_i}) + R - f_i \ell(\alpha) = R.$$

$$\iff \frac{\ell(\alpha_1) + \ldots + \ell(\alpha_{f_i})}{f_i} = \ell(\alpha)$$

$$\iff \ell(\alpha_1) = \ldots = \ell(\alpha_{f_i}) = \ell(\alpha).$$

$\iff \ell[a_1] = \cdots = \ell[a_{f_i}] = \ell[\alpha]$.

$\Rightarrow$ ensures consistency.

$(M = fB,\ N = 2^B)$

$(R = M^{\alpha(1/\varepsilon)} - N^{1/\varepsilon} = (fB)^{\alpha(1/\varepsilon)} \cdot (2^B)^{1/\varepsilon})$

Runtime: numbers have # bits

$$\simeq \frac{n}{B} \cdot \log R + \frac{m}{B} + \frac{n}{B} + O(\log(m+n))$$

$$= \frac{n}{B} \cdot \left(O\left(\frac{1}{\varepsilon} \log fB\right) + (1+\varepsilon)B \right) + \frac{m}{B} + \frac{n}{B} + O(\log(m+n))$$

$$= (1+\varepsilon)n + O\left(\frac{1}{\varepsilon} \frac{n}{B} \log(fB) + \frac{m}{B}\right)$$

Set $B = \frac{100}{\varepsilon^3}$

$$\approx (1+\varepsilon)n$$

$$\Rightarrow t \lesssim 2^{(1+\varepsilon)n} \qquad m \le g(n)$$

$$\#\text{numbers} \le O\left(m \cdot (2^B)^{kB} + n \cdot 2^B\right)$$

$$= O(n) \quad \text{for const } f, k, \varepsilon$$

$\Rightarrow$ total time $T\left(O(n),\ 2^{(1+\varepsilon)n}\right)$

$$\le \left(2^{(1+\varepsilon)n}\right)^{1-\delta} \cdot 2^{o(n)}$$

$$\lesssim 2^{\left(1-\frac{\delta}{2}\right)n}$$

by setting $\varepsilon = \delta/2$

□

Problem: Boolean Orthogonal Vectors (OV)

Given sets A, B of n vectors in $\{0,1\}^d$, decide if $\exists a \in A, b \in B$ s.t.

$$a \cdot b = 0$$

$$= \sum_{i=1}^{d} a[i] \cdot b[i]$$

naive alg'ms: $O(dn^2)$ time

or $O(M(n,d,n))$ time

$\leq O(d^{\omega-2} n^2)$ $\quad (d \leq n)$

beat n^2??

$\begin{cases} O(d \cdot 2^d n) \text{ time} \\ O(n + d \cdot 4^d) \end{cases}$ good only when $d = o(\log n)$

$n^{2 \cdot o(1)}$

OPEN: $O(n^{2-\delta})$ for $d = \omega(\log n)$??

OV Conjecture No alg'm for OV in $O(d^{O(1)} n^{2-\delta})$ time.

Thm (Williams '05)

SETH Conj $\Rightarrow$ OV Conj.

Pf: Reduce c-sparse k-SAT $\longrightarrow$ OV.

Suppose OV could be solved in $T(n,d) = O(d^{O(1)} n^{2-\delta})$ time.

Suppose OV ... time.

Given c-sparse k-CNF formula F
with n vars $x_1, \ldots, x_n$ & m clauses $C_1, \ldots, C_m$,
$(m \le cn)$.

For each assignment φ
of $x_1, \ldots, x_{n/2}$,

define vector $a_\varphi \in \{0,1\}^m$.
where $a_\varphi[j] = 0$ iff C_j satisfied by φ.

For each assignment ψ
of $x_{n/2+1}, \ldots, x_n$,
define vector $b_\psi \in \{0,1\}^m$
where $b_\psi[j] = 0$ iff C_j satisfied by ψ

Solve OV on these 2 sets of $N = 2^{n/2}$ vectors
of dim $m \le cn$

Correctness: $\exists$ sat assignment for F

$\Leftrightarrow$ $\exists\, \varphi, \psi$ s.t.
$\forall j$, C_j is satisfied by φ or by ψ

$\Leftarrow$ $\exists\, \varphi, \psi$ s.t.,
$\forall j$, $a_\varphi[j] = 0$ or $b_\psi[j] = 0$

$\Leftarrow$ $\exists\, \varphi, \psi$ s.t.
$$\sum_{j=1}^{m} a_\varphi[j] \cdot b_\psi[j] = 0.$$

OV !!

$(x_1 \vee x_2) \wedge (x_5 \vee \bar{x}_6)$

Total time: $T(2^{n/2}, cn)$

$$
\begin{aligned}
& T(2^{\cdot}, \underline{\underline{cn}}) \\
&= O\left((cn)^{O(1)} \cdot \left(2^{n/2}\right)^{2-\delta}\right) \\
&= O^*\left(2^{(1-\delta/2)n}\right).
\end{aligned}
$$

□