Complexity of Lattice Problems: A Cryptographic Perspective
Daniele Micciancio, Shafi Goldwasser

The 32th HISS
2011/8/26
JAIST

Chapter 6: Low-degree Hypergraph

Kai Yuen Cheong
Miyaji Lab, JAIST

Purpose of this chapter

- Prove Theorem 4.6 from Chapter 4
- Independent from the rest of the book
- The theorem is first stated in lattice form
- But it is more natural to present in terms of hyper-graph
- In this talk, we
  - Introduce and use hyper-graphs
  - Prove two related theorems
  - Prove the main theorem

The theorem in lattice form

- The main theorem: if we have
  - A set Z of binary vectors in $\{0,1\}^k$
  - Each vector has exactly h ones, k-h zeros
  - An integer n<k and a small ε
  - Fulfilling the condition

$$|Z| \geq h!\,k^{4\sqrt{h}n/\varepsilon}$$

The theorem in lattice form

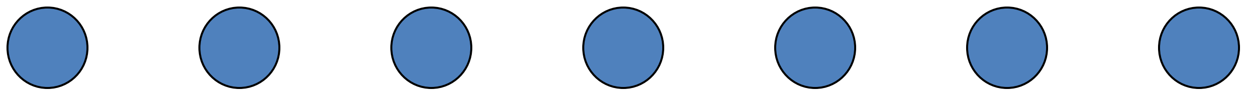
- Then:
  - There exists a binary matrix T in $\{0,1\}^{n \times k}$
  - Such that $$\{0,1\}^n \subseteq T(Z) = \{Tz : z \in Z\}$$
  - Moreover, if T is randomly chosen such that each element is 1 with probability $\varepsilon/(4hn)$
  - Then the event happens with probability at least $1-6\varepsilon$

Hyper-graph

- Graph: {V,E}
  - V: a set of vertices
  - E: a set of edges e, where each e must be a set of two vertices
- Hyper-graph: {V,Z}
  - V: set of vertices
  - Z: the set of hyper-edge z, where z can be any subset of V
- Regular hyper-graph
  - For each z in Z, the size |z| is the same
  - All hyper-edges contains the same number of vertices
  - h=|z| is called the degree of regular hyper-graph

Hyper-graph representation

V



Z

0	1	1	0	1	0	0
1	1	0	0	1	0	0
0	1	1	0	0	0	1
0	0	1	0	1	0	1
0	1	0	0	1	1	0
0	0	1	1	0	0	1

The theorem in hyper-graph

- Let (V,Z) be a regular hyper-graph, degree h, and |V|=k
- Let T=(T_1,…T_n) be a sequence of random subsets of V
  - Where in each T_i elements of V are picked independently with probability ε/(4hn)
- Let U be any subset of V, define

$$T(U) = (|T_1 \cap U|, |T_2 \cap U|, \ldots |T_n \cap U|)$$

The theorem in hyper-graph

- Define

$$T(Z) = \{T(U) : U \in Z\}$$

- The theorem:
  - If $|Z| \geq h! k^{4\sqrt{h} n / \varepsilon}$
  - Then $\{0,1\}^n \subseteq T(Z)$
  - with probability at least 1-6ε

Warm up before proving the main theorem

- Sauer's Lemma
  - (Lemma 6.1, 6.2)
- Weak version of the main theorem
  - (Lemma 6.3-6.7, Theorem 6.8)

Sauer's Lemma

- It is a warm up for the main theorem, by assuming that each T_i only contains one element of V
- Let G be a subset of V, define

$$Z\Big|_G = \{A \bigcap G : A \in Z\}$$

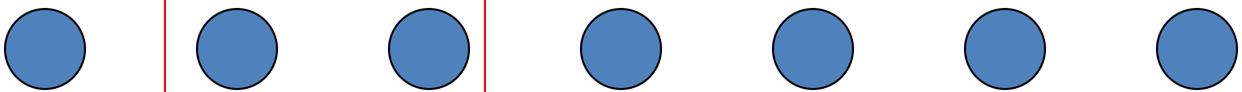
- Define the number of choices for choosing at most n from k elements as

$$[k,n] = \sum_{i=0}^{n} \binom{k}{i}$$

Sauer's Lemma (6.1)

- If $|Z| \geqslant [k,n]$ then there exists a G of size n such that $Z|_G$ is the power set of G

V



Z

0	1	1	0	1	0	0
1	1	0	0	1	0	0
0	1	1	0	0	0	1
0	0	0	1	1	0	1
0	1	0	0	1	1	0
0	0	1	1	0	0	1

G

Sauer's Lemma

- The proof is done by induction
  - Case for [k,k]=2^k is trivial
  - Case for [k,0]=1 is trivial
- Assume the Lemma holds for [k-1,n], [k-1,n-1], we show for the case [k,n]

Sauer's Lemma

- Pick an element a from V and define U=V¥{a}
- Define

$$Z_0 = \{A \subseteq U : A \in Z\}$$

$$Z_1 = \{A \subseteq U : A \bigcup \{a\} \in Z\}$$

Hyper-graph representation

							a
V	●	●	●	●	●	●	●
Z_0	0	1	1	0	1	0	0
	1	1	0	0	1	0	0
Z_1	0	1	1	0	0	0	1
	0	0	1	0	1	0	1
	0	0	0	0	1	1	1
	0	0	1	1	0	0	1

Sauer's Lemma

- Note that [k,n]=[k-1,n]+[k-1,n-1]
- So

$$\left|Z_0 \cup Z_1\right| + \left|Z_0 \cap Z_1\right| = \left|Z\right|$$
$$\geq [k, n]$$
$$= [k-1, n] + [k-1, n-1]$$

- Therefore either $\left|Z_0 \cup Z_1\right| \geq [k-1, n]$
- or $\left|Z_0 \cap Z_1\right| \geq [k-1, n-1]$

Sauer's Lemma

- If $\left|Z_0 \bigcup Z_1\right| \geq [k-1, n]$
- Then there exists G, a subset of U, with |G|=n, such that $(Z_0 \bigcup Z_1)\big|_G$
  is the power set of G (by induction assumption on [k-1,n] with |U|=k-1, |G|=n)
- Moreover $(Z_0 \bigcup Z_1)\big|_G = Z\big|_G$
  - Since $a \notin G$

Sauer's Lemma

- If $\left|Z_0 \cap Z_1\right| \geq [k-1, n-1]$
- Then there exists G' such that $(Z_0 \cap Z_1)\big|_{G'}$ is the power set of G'
- This is from inductive hypothesis, so we can only say that |G'|=n-1
- We set $G = G' \cup \{a\}$
  - Let A be any subset of G
  - A¥{a} is in both $Z_0|_{G'}$ and $Z_1|_{G'}$
  - A is in $Z|_G$

Sauer's Lemma (6.2)

- Since $[k,n]<k^n$
- We get this corollary
  - Let Z be a subset of $\{0,1\}^n$, if $|Z| \geqslant k^n$ then there exists a matrix T in $\{0,1\}^{n \times k}$
  - such that $\{0,1\}^n \subseteq T(Z)$
  - Elements of Z need not be binary vectors of the same Hamming weight

The weak theorem

- It is the foundation of the strong theorem
- Purpose of the weak theorem:
  - For the given hyper-graph (V,Z)
  - A given x in $\{0,1\}^n$
  - And a random T
  - The probability that x is not in T(Z) is bounded
- There are three steps in the proof
  - Step 1: Exponential bound
  - Step 2: Investigate well spread properties
  - Step 3: Proof of the weak theorem

Step 1: Exponential bound

- Lemma 6.3
  - Let x be a given binary vector in $\{0,1\}^n$
  - Let U,U' be two subsets of V of size d
    - While size of intersection of U,U' is r
  - Let $T=(T_1,\dots T_n)$ be sequence of subsets of V
    - For each T_i, each element of V is picked independently with probability p
  - Then probability that x=T(U)=T(U') is

$$\Phi(r) = (1-p)^{(2d-r)n}\left(\frac{pr}{1-p}+\left(\frac{p(d-r)}{1-p}\right)^2\right)^{\|x\|_1}$$

Where $||x||_1$ denotes Hamming weight

Exponential bound

- Proof of Lemma 6.3
  - Since T_i are chosen independently

$$\Pr[T(U) = T(U') = x] = \prod_{i=1}^{n} \Pr[|T_i \cap U| = |T_i \cap U'| = x_i]$$

  - We try to show that

$$\Pr[|T_i \cap U| = |T_i \cap U'| = x_i] = (1-p)^{2d-r}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right)^{x_i}$$

Proof of Lemma 6.3

- For x_i=0 it is

$$\Pr[|T_i \cap U| = |T_i \cap U'| = 0] = (1-p)^{|U \cup U'|} = (1-p)^{2d-r}$$

  – For T_i picking no elements from U or U’

- For x_i=1, that is $|T_i \cap U| = |T_i \cap U'| = 1$
  – T_i has 1 element from intersection of U and U’
  – or T_i has 1 element from U¥U’ and 1 element from U’¥U

Proof of Lemma 6.3

- Probability of the first case

$$\left|U \cap U'\right| \cdot p(1-p)^{\left|U \cup U'\right|-1} = (1-p)^{2d-r}\left(\frac{pr}{1-p}\right)$$

- Probability of the second case

$$\left|U \setminus U'\right| \cdot \left|U' \setminus U\right| \cdot p^2(1-p)^{\left|U \cup U'\right|-2} = (1-p)^{2d-r}\left(\frac{p(d-r)}{1-p}\right)^2$$

- These two cases are mutually exclusive

Proof of Lemma 6.3

- Therefore we get the sum

$$\Pr[|T_i \cap U| = |T_i \cap U'| = 1] = (1-p)^{2d-r}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right)$$

- Thus

$$\Pr[|T_i \cap U| = |T_i \cap U'| = x_i] = (1-p)^{2d-r}\left(\frac{pr}{1-p} + \left(\frac{p(d-r)}{1-p}\right)^2\right)^{x_i}$$

Corollary 6.4

- Set U=U' we have

$$\Pr_T[T(U) = x]$$

$$= \Phi(d)$$

$$= (1-p)^{dn}\left(\frac{pd}{1-p}\right)^{\|x\|_1}$$

Exponential bound

- Proposition 6.5
  - Let (V,Z) be a regular hyper-graph, degree d
  - Let $T=(T_1,\dots T_n)$ as defined before, using probability p
  - U,U' chosen randomly from Z
- Then

$$\Pr[x \notin T(Z)] \le \underset{R}{E}[e^{\theta R}] - 1$$

where

$$\theta = \frac{np}{1-p} + \frac{n}{pd^2}$$

$$R = |U \cap U'|$$

Proof of Proposition 6.5

- Define indicator X_U=1 if T(U)=x and X_U=0 otherwise
- Define $X=\Sigma X_U$ for all U in Z
- X=0 if and only if x is not in T(Z)
- $Pr[X=0] \leqslant Pr[|X-E[X]| \geqslant E[X]]$

  $\leqslant Var[X]/(E[X])^2$ (Chebyshev inequality)

Proof of Proposition 6.5

- To continue we compute E[X]

$$\mathop{E}_{T}[X] = \sum_{U \in Z} \mathop{E}_{T}[X_U] = \sum_{U \in Z} \Pr_{T}[T(U) = x] = |Z| \cdot \Phi(d)$$

- And E[X²]

$$\mathop{E}_{T}[X^2] = \mathop{E}_{T}[(\sum_{U \in Z} X_U)^2]$$

$$= \mathop{E}_{T}[\sum_{U,U' \in Z} X_U \cdot X_{U'}] = \sum_{U,U' \in Z} \Pr_{T}[T(U) = T(U') = x]$$

$$= |Z|^2 E[\Phi(R)]$$

Proof of Proposition 6.5

$$\Pr_T[x \notin T(Z)] \le \frac{\underset{R}{E}[\Phi(R)]}{\Phi(d)^2} - 1$$

$$= \underset{R}{E}[(1-p)^{-nR}\left(\frac{(1-p)R}{pd^2} + \left(1 - \frac{R}{d}\right)^2\right)^{\|x\|_1}] - 1$$

$$< \underset{R}{E}[(1+\frac{p}{1-p})^{nR}(\frac{R}{pd^2}+1)^n] - 1$$

Increase value of some terms

$$< \underset{R}{E}[e^{\frac{pnR}{1-p}} e^{\frac{nR}{pd^2}}] - 1$$

$(1+1/x)^x < e$

$$= \underset{R}{E}[e^{R\theta} - 1]$$

Step 2: Well spread hyper-graph

- The previous result depends on R
- We investigate R in this part through well spread hyper-graph
- Definition: (V,Z) is well spread if for all subset of V (denoted by W) of size at most d, the fraction of hyper-edges containing W is limited by

$$\frac{\left|\{U \in Z : W \subseteq U\}\right|}{|Z|} \leq \frac{1}{d(d-1)\ldots(d-|W|+1)} = \frac{(d-|W|)!}{d!}$$

Well spread hyper-graph

- Lemma 6.6
  - Let (V,Z) be a regular and well spread hyper-graph, degree d
  - Choose U and U' uniformly from Z independently
  - Let $R = |U \cap U'|$
  - Then for all r>0, we have

$$\Pr[R \geq r] < \frac{1}{r!}$$

Proof of Lemma 6.6

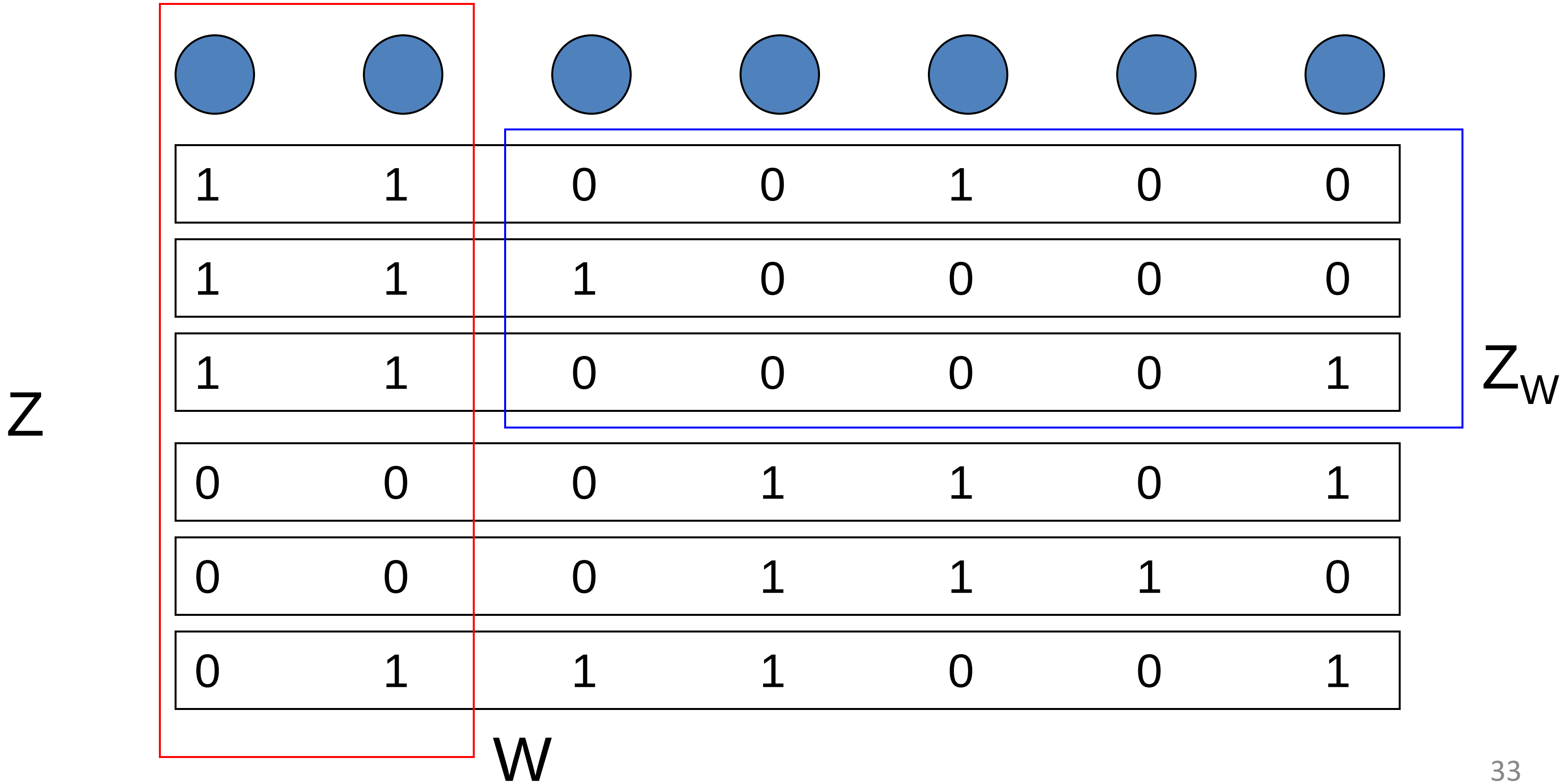
- Proof: in the following we can assume U is fixed while U' is random
  - If $|U \cap U'| \geq r$
  - Then U' contains a subset of U of size r
  - So $\Pr_{U'}[|U \cap U'| \geq r] \leq \sum_{W \in \binom{U}{r}} \Pr_{U'}[W \subseteq U']$

$$= \sum_{W \in \binom{U}{r}} \frac{|\{U' \in Z : W \subseteq U'\}|}{|Z|} \leq \binom{d}{r} \frac{(d-r)!}{d!} = \frac{1}{r!}$$

Well spread hyper-graph

- Definition: For any W which is subset of V, the induced hyper-graph is defined by

$$Z_W = \{U \subseteq V \setminus W : U \bigcup W \in Z\}$$



1	1	0	0	1	0	0
1	1	1	0	0	0	0
1	1	0	0	0	0	1
0	0	0	1	1	0	1
0	0	0	1	1	1	0
0	1	1	1	0	0	1

Well spread hyper-graph

- Properties of induced hyper-graphs
  - |Z| is well spread if for every W of size at most d,

$$|Z_W| \le \frac{(d-|W|)!}{d!}|Z|$$

  - Z_W is regular with degree d'=d-|W|, where d is degree of Z
  - If |W|=0 then $Z=Z_W$
  - If $W \cap W' = \phi$
    - Then $(Z_W)_{W'} = Z_{W \cup W'}$
    - Otherwise $(Z_W)_{W'}$ is empty

Lemma 6.7

- For any regular hyper-graph (V,Z) of degree h, there exists W such that (V, Z_W) is well spread, and
  $|Z_W| > |Z| / h!$
- Proof:
  - If (V,Z) is well spread, then set W to be empty (trivial case)
  - Otherwise (V,Z) is not well spread, by definition there is at least one W size at most h such that
    $$|Z_W| > \frac{(h-|W|)!}{h!}|Z|$$
  - Observe that this cannot be true for all W

Lemma 6.7

- Let W be maximal (of size) in all sets fulfilling the condition (choose any if there are more than one)
- $|Z_W|>|Z|/h!$ is obviously true
- Z_W is of degree $d=h-|W|$
- Next, for any U that is subset of V
  – If U is empty $|(Z_W)_U|=|Z_W|$
  – If U and W intersect then $|(Z_W)_U|=0$

Lemma 6.7

- Assume U is not empty and does not intersect with W

$$\left|\left(Z_W\right)_U\right| = \left|Z_{W\cup U}\right|$$

$$\le \frac{(h-|W\cup U|)!}{h!}|Z|$$

Maximality of W

$$= \frac{(h-|W|-|U|)!}{(h-|W|)!}\frac{(h-|W|)!}{h!}|Z|$$

$$< \frac{(d-|U|)!}{d!}|Z_W|$$

- This is true for any U, so Z_W is well spread

Step 3: The weak theorem

- Theorem 6.8: for sufficiently small ε, positive integer n and degree h hyper-graph (V,Z) such that $|Z| \geq h!|V|^{\sqrt{h}n/\varepsilon}$
- Choose $T=(T_1,\ldots T_n)$ where T_i are subsets of V picking elements of V independently with probability $p=\varepsilon/(hn)$
- Then for every x in $\{0,1\}^n$

$$\Pr[x \in T(Z)] > 1 - 5\varepsilon$$

Proof of theorem 6.8

- Lemma 6.7 says there is a W such that (V,Z_W) is well spread and also

$$|Z_W| \geq |Z| / h! > |V|^{\sqrt{h} n/\varepsilon}$$

- Let F be the event of having none of elements in W are in any of T_i
  - We have $\Pr[\sim F] \leqslant |W|np \leqslant hnp = \varepsilon$
- Also note that

$$\Pr_T[x \notin T(Z) \mid F] \leq \Pr_T[x \notin T(Z_W)]$$

Proof of theorem 6.8

- Let d be the degree of Z_W
- Since $|V|^{\sqrt{h}n/\varepsilon} < |Z_W| \le \binom{|V|}{d} < |V|^d$
- We have $d > \sqrt{h}n/\varepsilon$
- Next, with Proposition 6.5

$$\Pr_T[x \notin T(Z_W)] \le E[e^{R\theta}] - 1$$

- Where R is the size of intersection of two random elements in Z_W

Proof of theorem 6.8

$$\theta = \frac{np}{1-p} + \frac{n}{pd^2}$$

$$= \frac{\varepsilon}{h - \varepsilon / n} + \frac{hn^2}{\varepsilon d^2}$$ hnp=ε

$$< \frac{\varepsilon}{1-\varepsilon} + \frac{hn^2}{\varepsilon d^2}$$

$$< \frac{\varepsilon}{1-\varepsilon} + \varepsilon$$ $d > \sqrt{h} n / \varepsilon$

Proof of theorem 6.8

- Z_W is well spread, so Pr[R⩾r]<1/r!
- So

$$E[e^{R\theta}] = \sum_{r\geq 0} e^{r\theta} \Pr[R=r]$$

$$= \sum_{r\geq 0} e^{r\theta} (\Pr[R\geq r] - \Pr[R\geq r+1])$$

$$= \sum_{r\geq 0} e^{r\theta} \Pr[R\geq r] + \sum_{r\geq 1} e^{(r-1)\theta} \Pr[R\geq r]$$

$$= 1 + (1-e^{-\theta}) \sum_{r\geq 1} e^{r\theta} \Pr[R\geq r]$$

$$< 1 + \theta \sum_{r\geq 1} \frac{e^{r\theta}}{r!}$$

Because $1-e^{-x}<x$

$$= 1 + \theta (e^{e^{\theta}} - 1)$$

Proof of theorem 6.8

$$\Pr[x \notin T(Z)]$$

$$= \Pr[x \notin T(Z) \mid F]\Pr[F] + \Pr[x \notin T(Z) \mid \overline{F}]\Pr[\overline{F}]$$

$$\leq \Pr[x \notin T(Z) \mid F] + \Pr[\overline{F}]$$

$$\leq \varepsilon + \theta(e^{e^{\theta}} - 1)$$

$$< \varepsilon + \varepsilon(1 + \frac{1}{1-\varepsilon})(e^{e^{\varepsilon(1+\frac{1}{1-\varepsilon})}} - 1)$$

$$< 5\varepsilon$$

$$(1 - \frac{1}{1-\varepsilon}) \rightarrow 2$$

$$e^{e^{\theta}} \rightarrow e \approx 2.7$$

For sufficiently small ε

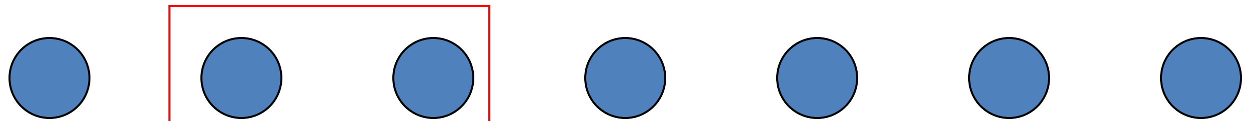
The final theorem

- The weak theorem is only about bounding the probability of failure for one x
- Before the proving the final theorem, we need the following probabilistic version of Sauer's Lemma
- Lemma 6.9: Let |V|=n. Let W be a set of hyper-edges and G is uniformly selected from all subsets of V, and ρ(G) is the power set of G, then

$$\Pr_G[W|_G = \rho(G)] \geq \frac{|W|}{2^n}$$

Hyper-graph illustration

V



W

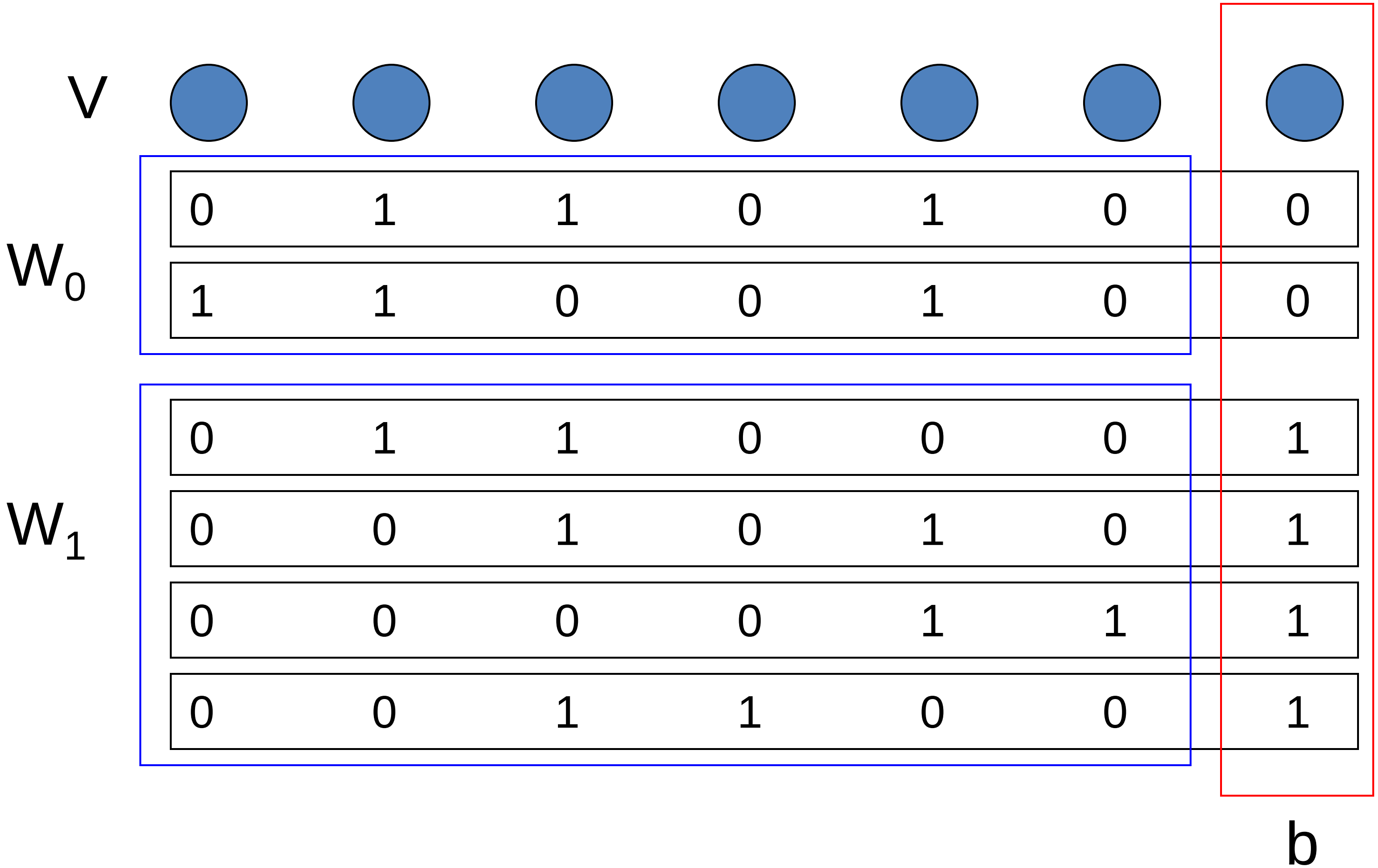
0	1	1	0	1	0	0
1	1	0	0	1	0	0
0	1	1	0	0	0	1
0	0	0	1	1	0	1
0	1	0	0	1	1	0
0	0	1	1	0	0	1

G

Proof of Lemma 6.9

- Proof is by induction on n, which is trivial for n=0. If the statement is true for n, add a new element b to V
- For any hyper-graph (V,W)
- Define W_0 and W_1 same as Lemma 6.1 based on b
- Select G, define G’=G¥{b}

Hyper-graph representation



Proof of Lemma 6.9

- If b is not in G and $(W_0 \cup W_1)\big|_{G'} = \rho(G')$
  - Then $W|_G = \rho(G)$
- If b is in G and $(W_0 \cap W_1)\big|_{G'} = \rho(G')$
  - Then $W|_G = \rho(G)$ too
- These two events are mutually exclusive
- And b is in G with ½ chance
- Also, induction hypothesis can be applied on W_0 and W_1

Proof of Lemma 6.9

$$\Pr[W\big|_G = \rho(G)]$$

$$\geq \frac{1}{2}\Pr[(W_0 \bigcap W_1)\big|_{G'} = \rho(G')] + \frac{1}{2}\Pr[(W_0 \bigcup W_1)\big|_{G'} = \rho(G')]$$

$$\geq \frac{1}{2}\left(\frac{\left|W_0 \bigcap W_1\right|}{2^n}\right) + \frac{1}{2}\left(\frac{\left|W_0 \bigcup W_1\right|}{2^n}\right)$$

$$= \frac{\left|W\right|}{2^{n+1}}$$

Finally… (Theorem 4.6)

- The trick is to use a larger T' in $\{0,1\}^{4n \times k}$ and then shrink it
- Each entry is 1 with probability p=e/(4hn)
- Next, choose a random G as subset of {1,…4n}
- If |G|⩾n, set T as the n by k matrix using rows of T' selected by first n elements of G
- If |G|<n, then select T randomly
- The change is only mental
  – Distribution of T is unchanged

Proof of theorem 4.6

- Define $W = T'(Z) \bigcap \{0,1\}^{4n}$
- If |G|⩾n and $\{0,1\}^{|G|} \subseteq W\big|_G$
  - Then $\{0,1\}^n \subseteq T(Z)$

W

0	1	1	0	1	0	0
1	1	0	0	1	0	0
0	1	1	0	0	0	1
0	0	0	1	1	0	1
0	1	0	0	1	1	0
0	0	1	1	0	0	1

G

Proof of theorem 4.6

- We investigate separately the probability of |G|<n and $\{0,1\}^{|G|} \subseteq W\big|_G$
- Note that E[|G|]=2n and Var[|G|]=n from binomial distribution
- For sufficiently large n, using Chebyshev inequality

$$\Pr[|G| < n] < \Pr[||G| - E[|G|]| < n] < \frac{1}{n} < \varepsilon$$

Proof of theorem 4.6

$$\Pr_{G,T'}[\{0,1\}^{|G|} \subseteq W\big|_G]$$

$$= \underset{T'}{E}[\Pr_G[\{0,1\}^{|G|} \subseteq W\big|_G]]$$

$$\geq \underset{T'}{E}[\frac{|W|}{2^{4n}}]$$ Lemma 6.9

$$= \underset{T'}{E}[\Pr_{x \in \{0,1\}^{4n}}[x \in W]]$$

$$= \underset{x \in \{0,1\}^{4n}}{E}[\Pr_{T'}[x \in T'(Z)]]$$

$$\geq \min_{x \in \{0,1\}^{4n}} \Pr_{T'}[x \in T'(Z)]$$

$$\geq 1 - 5\varepsilon$$ Theorem 6.8

Proof of theorem 4.6

- So $\Pr[|G| < n] < \varepsilon$
- And $\Pr_{G,T'}[\{0,1\}^{|G|} \not\subset W|_G] < 5\varepsilon$
- Therefore the probability that T satisfies theorem 4.6 is at least 1-6ε

Thank you very much for listening

Q&A session