Blockcourse on High-Dimensional Computational Geometry	Summer 2013

Lecture 4 — July 25, 2013

Helmut Alt *Scribes: Michal Kleinbort and Sylvie Temme*

Definition 1. *(#LEXT)*
given: a partial order (by Hasse diagram)
compute: # of linear extensions

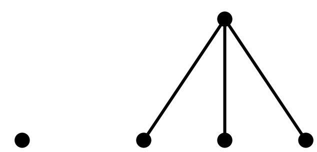

Figure 1: The number of linear extensions for this partial order is 30

Theorem 2. *(Brightwell, Winkler, 1991)*
#LEXT is #P-complete.

Proof. We will proof the theorem by reduction from #SAT.
Let I be an Instance for #SAT with m variables and n clauses. Let $M = 7n + m$.
Define the partial order P_I:

- for each variable x there is a vertex h_x
- for each clause c there are 7 vertices $c_1, \ldots, c_7$
- if c has variables x, y, z (negated or not), then the vertices in P_I are connected as in figure 2

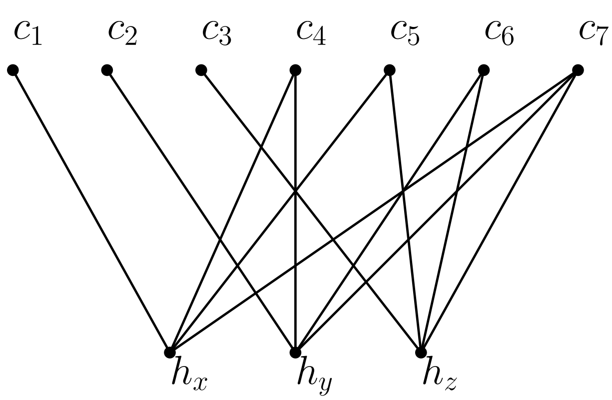

Figure 2: The relations in P_I corresponding to a clause c involving the variables x, y, z

P_I has size M.
Let L_I be the number of linear extensions of P_I. We can determine L_I by a call to #LEXT-oracle

$\boldsymbol{O}(M)$, where $\boldsymbol{O}(M)$ denotes an oracle call to partial order of size M.
Let $S_0 = \left\{ p \,|\, p \text{ prime}, M < p < M^2 \right\}$. Then

$$\prod S_0 \overset{\text{excercise}}{\geq} M! \cdot 2^M > M! \cdot 2^m$$

Let $S = \{ p \in S_0 \,|\, p \nmid L_I \}$, then

$$\prod S > 2^m$$

since $L_I \leq M!$

Let $S(I)$ be the number of satisfying assignments for I.
idea:

$$\text{compute} \quad S(I) \bmod p \quad \text{for all } p \in S$$

From those values:

$$\text{compute } \ S(I) \ \text{ by Chinese remainder theorem}$$

For each $p \in S$, construct a partial order $Q_I(p)$ as in figure 3:

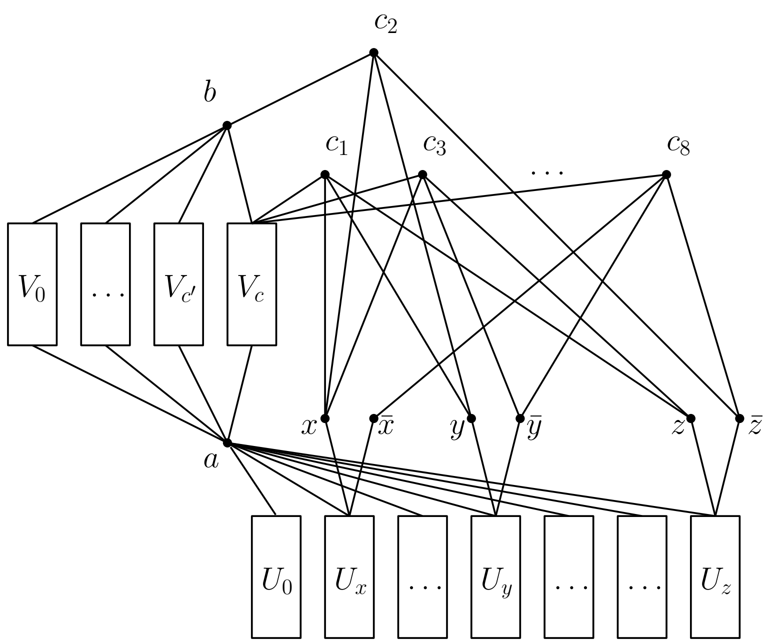

Figure 3: The partial order $Q_I(p)$. The rectangles represent antichains of size $p-1$. The only clause vertices shown here are those corresponding to the clause $c = x \vee y \vee \bar{z}$

- the U_i and V_j are antichains of $p-1$ vertices each

- there is a box U_i for each variable and a box V_j for each clause and additionally U_0 and V_0
- the vertices for x, $\bar{x}$, y, $\bar{y}$, z, $\bar{z}$ etc. are called *literal vertices*
- the vertices for the c_i are called *clause vertices*
- each clause vertex corresponds to an assignment for x, y, z and is connected to the three literals (of the variables in clause c) that are TRUE in this assignment
- the one clause vertex above b is the one that is connected with the literals of c
- the part shown in the figure for the clause $c = x \vee y \vee \bar{z}$ is constructed for each clause c.

A linear extension "$\leq$" of $Q_I(p)$ has the form:

$$\underbrace{B}_{\text{bottom part}} \leq a \leq \underbrace{M}_{\text{middle part}} \leq b \leq \underbrace{T}_{\text{top part}}$$

Let φ be a configuration B^φ, M^φ, T^φ of $Q_I(p)$ into B, M, T.
If P^φ, the partial order according to φ, extends $Q_I(p)$, then the number of linear extensions of $Q_I(p)$

$$N\left(Q_I(p)\right) = \sum_{\text{conf } \varphi} N\left(P^\varphi\right)$$

and

$$N\left(P^\varphi\right) = N\left(P_B^\varphi\right) \cdot N\left(P_M^\varphi\right) \cdot N\left(P_T^\varphi\right)$$

where P_B^φ is the bottom part of P^φ, P_M^φ the middle part and P_T^φ the top part.

Definition 3. *A configuration φ is called **feasible**, iff*

$$p \nmid N\left(P_B^\varphi\right)\ ,\ p \nmid N\left(P_M^\varphi\right)$$

Lemma 4. *Let φ be a feasible configuration for $Q_I(p)$.*

(a) B^φ contains exactly one literal vertex per variable and

$$N\left(P_B^\varphi\right) = \frac{(p\,(m+1)-1)!}{p^m} \not\equiv 0 \mod p$$

(b) M^φ contains no literal vertex and exactly one clause vertex per clause and

$$N\left(P_M^\varphi\right) = \frac{(p\,(n+1)-1)!}{p^n} \not\equiv 0 \mod p$$

Proof. (a) φ feasible $\Rightarrow P_B^\varphi$ contains antichain $U = U_0 \cup \bigcup U_x$ of size $(p-1)(m+1)$.
Within the bottom part B^φ: U_0 is isolated and for every x U_x is isolated if x and $\bar{x}$ are not in B^φ. Suppose $\exists$ one isolated $U_x \Rightarrow r \geq p-1$ isolated vertices in B^φ. In a linear extension of B^φ: $k \cdot (k-1) \cdot \ldots \cdot (k-r+1)$ possibilities to place them (where $k = |B^\varphi|$). This number must divide $N\left(P_B^\varphi\right)$. Since φ is feasible $\Rightarrow p \nmid N\left(P_B^\varphi\right) \Rightarrow$ no multiple of p is a factor in the product $k \cdot (k-1) \cdot \ldots \cdot (k-r+1)$. It follows:

1. $r = p - 1$
2. for each variable x: the vertex/vertices for x or for $\bar{x}$ are in B^φ
3. $k \equiv -1 \mod p$

For k' = number of literal vertices in B^φ:

$$\begin{aligned} k &= \underbrace{(p-1)(m+1)}_{U\text{-blocks}} + k' \quad \mid \text{take} \mod p \\ -(m+1) + k' &\equiv -1 \mod p \\ -m + k' &\equiv 0 \mod p \\ k' &\equiv m \mod p \end{aligned}$$

Since $p > m$ and $m \overset{2.}{\leq} k' \leq 2m$,

$$k' = m$$

i.e., exactly one literal vertex per variable is in B^φ.
P_B^φ looks like in figure 4.

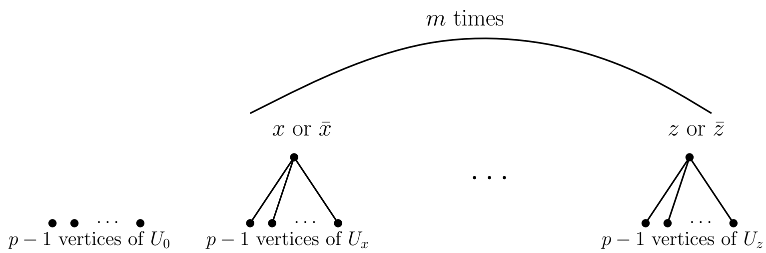

Figure 4: P_B^φ

With problem three from the third problem set follows:

$$N\left(P_B^\varphi\right) = \frac{(p\,(m+1)-1)!}{p^m}$$

In the numerator, there is m times the factor p, and this is divided by p^m, therefore there is no more multiple of p in the number.
(b) excercise! □

Lemma 5. *The number $S(I)$ of satisfying assignments of I = the number of feasible configurations of $Q_I(p)$ for any $p \in S$.*

Proof. We construct a mapping h : assignments $\rightarrow$ configurations as follows:
given an assignment α, construct configuration $\varphi = h(\alpha)$:

- the literal vertices for the literals that are satisfied are placed in T^φ and the others in B^φ

- the clause vertices $c_1, \ldots, c_8$ corresponding to literal combinations whose $\vee$ is 1 (TRUE) are placed in T^φ, the others in M^φ

- (U_x in B^φ, V_c in M^φ)

Claim 6. *α is satisfying for $I \Leftrightarrow h(\alpha)$ is feasible*

Proof. "$\Leftarrow$": $\varphi = h(\alpha)$ is feasible $\overset{L.4(a)}{\Rightarrow}$ for each variable x one literal h_x is in T^φ and the other, l_x, is in B^φ, by construction: $\alpha(h_x) = 1$ and $\alpha(l_x) = 0$. We have to show that α is satisfying. Assume, α is not, there exists a clause C that is not satisfied. The literals in C are all set to FALSE by α, therefore the clause vertex c_i, which corresponds exactly to the literals of C is placed in M^φ (by construction of h). So it's not above b. $\lightning$
"$\Rightarrow$": look at proof of Lemma 4. □

h restricted to satisfying assignments is a bijection to the feasible configurations. We show that the inverse mapping h^{-1} exists: by Lemma 4: for each variable one literal h_x is placed in T^φ, the other, l_x, in B^φ. So $\alpha(h_x) = 1$. Therefore, α is a satisfying assignment, because if not, one clause C is not satisfied, then ... (as above) $\lightning$

□

<u>Observation</u>: φ feasible $\Rightarrow P_T^\varphi$ has 7 clause vertices, each one is above at least one of h_x, h_y, h_z. $\Rightarrow P_T^\varphi$ is isomorphic to P_I from the beginning, see figure 2.
It follows:

$$\begin{aligned} N\left(P^\varphi\right) &= N\left(P_B^\varphi\right) \cdot N\left(P_M^\varphi\right) \cdot N\left(P_T^\varphi\right) \\ &= \frac{(p\,(m+1)-1)!}{p^m} \cdot \frac{(p\,(n+1)-1)!}{p^n} \cdot L_I \qquad =: N_0 \end{aligned}$$

Since if φ is not feasible, then $N\left(P^\varphi\right)$ has p as a factor, it follows:

$$\begin{aligned} N\left(Q_I(p)\right) &\equiv \sum_{\varphi \text{ feasible}} N\left(P^\varphi\right) \mod p \\ &\equiv N_0 \cdot (\#\text{ feasible configurations of } Q_I(p)) \mod p \\ &\overset{L.5}{\equiv} N_0 \cdot S(I) \mod p \quad \text{for all } p \in S \end{aligned}$$

From this: determine $S(I)$ mod p:

- compute N_0 by one oracle call to determine L_I; the other terms in the definition of N_0 can be computed in polynomial time

- compute $\underbrace{N_0^{-1}}_{\text{standard techniques}} \cdot \underbrace{N\left(Q_I(p)\right)}_{\text{oracle call } \boldsymbol{O}(M^3)} \equiv S(I) \mod p$

So for each $p \in S$: determine $S(I)$ mod p this way. For this values determine $S(I)$, since

$$\prod_{p \in S} p \overset{\text{seen before}}{>} 2^m = \#\text{ all possible assignments } \geq S(I),$$

by chinese remainder theorem.

Chinese remainder theorem (Sun Tzu, 3rd century A.D.)
Suppose $p_1, \ldots, p_k$ are (pairwise relatively) prime. Then the congruence equalities

$$\begin{aligned} x &\equiv a_1 \mod p_1 \\ x &\equiv a_2 \mod p_2 \\ &\vdots \\ x &\equiv a_k \mod p_k \end{aligned}$$

have exactly one solution $x \in \{0, \ldots, p_1 \cdot p_2 \cdot \ldots \cdot p_k - 1\}$.

All computations are done with numbers whose size (# of bits) is polynomial in M:

$$\text{largest number: } N\left(Q_I(p)\right) \leq \left(O\left(M^3\right)\right)! < \left(cM^3\right)^{cM^3} \text{ for some constant c}$$

$$\text{\# of bits: } \leq \log\left(\left(cM^3\right)^{cM^3}\right) = O\left(M^3 \log M^3\right)$$

□

Definition 7. *(VCP)*
Given a convex polytope (H-polytope)
Compute its volume

Theorem 8. *VCP is #P-hard.*

Proof. We will proof the theorem by reduction from #LEXT.
Let π be a partial order on elements $x_1, x_2, \ldots, x_d$.
The *order polytope* of the partial order *pi* is defined as an intersection of the following set of halfspaces:

$$\{x_i - x_j \geq 0 | (x_i, x_j) \in \pi\}$$

where $0 \leq x_i \leq 1$ for all $i = 1, 2, \ldots, d$.
A linear extension satisfies $0 \leq x_{i_1} \leq x_{i_2} \leq \ldots \leq x_{i_d} \leq 1$ so that the partial order is preserved. Each inequality defines a halfspace and all these $d+1$ inequalities define the intersection of $d+1$ halfspaces which is a simplex in $\mathbb{R}^d$.
All these simplices have the same volume and their interiors are disjoint. That is, they do not intersect but may share boundaries. Their union is the order polytope itself.
Therefore:

$$\begin{aligned} \text{Vol(order polytope)} &= \text{\#simplices} \cdot \text{Vol(one simplex)} \\ &= (\text{\# linear extensions of } \pi) \cdot \frac{1}{d!} \end{aligned}$$

We can compute the number of linear extensions of a partial order π by an oracle call to VCP.

$$\Downarrow$$

$$\text{\#LEXT} \underset{\textit{reducible}}{\leq} \text{VCP}$$

□