2018-04-17 Danny Nguyen

- $\bar{t} = (t_1, \ldots, t_n)$
- $f(\bar{t}) = \sum_{i=0}^{I} c_i \frac{\bar{t}^{\bar{a}_i}}{\prod_j (1 - \bar{t}^{\bar{b}_{ij}})}$, $c_i \in \mathbb{Q}$, $\bar{a}_i, \bar{b}_{ij} \in \mathbb{Z}^n$, short G.F. (rational function)
- Length: $l(f) = \sum \lceil \log p_i \rceil + \lceil \log q_i \rceil + \lceil \log a_{ik} \rceil + \lceil \log b_{ij} \rceil$.
- Problem: Given a polytope $P = \{\bar{x} \in \mathbb{R}^n, A\bar{x} \leq \bar{b}\}$.
  Count $\# P \cap \mathbb{Z}^n$ in poly time (w.r.t. $A, \bar{b}$).
- Note: If dim n is unbounded, $\rightarrow$ hopeless (#P-complete) (hardest)

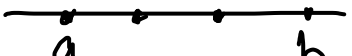
Thm (Barvinok '93)

We can compute:

$$f_P(\bar{t}) := \sum_{\bar{x} \in P \cap \mathbb{Z}^n} \bar{t}^{\bar{x}}$$

as a short G.F. (*) in poly time.

Then $|P \cap \mathbb{Z}^n| = \lim_{t \to 1} f_P(t)$.

- Ex: $P = \{a \le x \le b\}$ 

→ days

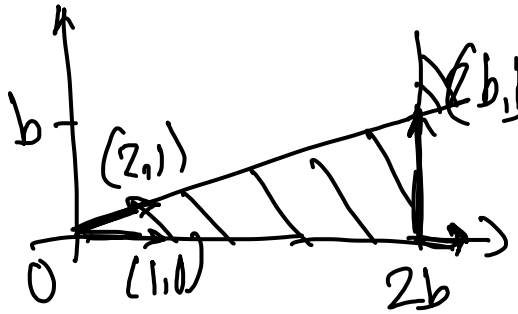
How to enumerate the points:

1st try: $f_P(t) = t^a + t^{a+1} + \dots + t^b$ → length exp. in $\log(a) + \log b$

2nd try: $= \frac{t^a}{1-t} + \frac{t^{b+1}}{1-t}$ → n in $\log(a) + \log b$ ✓

(use geo. sums)

- Ex2: → use cones (signed decomp. of cones)



$$\frac{1}{(1-t_1)(1-t_1^2 t_2)} - \frac{t_1^{2b}}{(1-t_1)(1-t_2)} + \frac{t_1^{2b} t_2^b}{(1-t_1^2 t_2)(1-t_2)}$$

- For us: Abstract away from geo. setting.

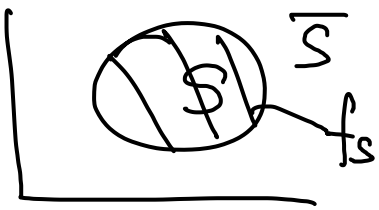
Consider $\{f\}$ all gen. func.'s f. What nice properties do they have?

e.g. $\{$short G.F.$\} \supsetneq$ Polytope.

First, assume our short G.F.'s are supported on $\mathbb{N}^n$:

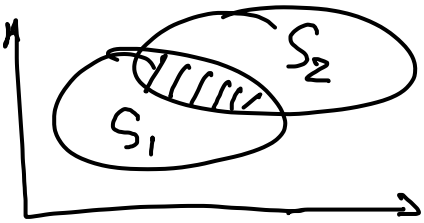
$f(\bar{t})$ expands $\sum_{\bar{x} \in S} \bar{t}^{\bar{x}}$, $S \subseteq \mathbb{N}^n$.

- Problem : Given f_S, can we compute $f_{\overline{S}}$?



$$\rightsquigarrow f_{\overline{S}}(t) = \underbrace{\prod_{i=1}^{n} \frac{1}{(1-t_i)}}_{\text{whole quarter plane}} - f_S(t)$$

- Now



Can we compute $f_{S_1 \cap S_2}(t)$ in poly time ?

Easy if S_1, S_2 are polytopes.

General sets : Answer is yes → (Bouvrinck & Zinovyev-Stein).

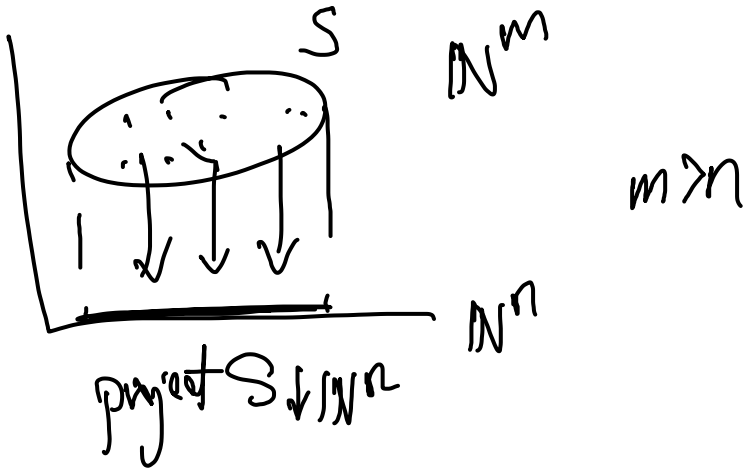
Trick : Do it term wise (Hadamard product) then add them back together.

→ All this depends on a general operator from Logic :

Projection

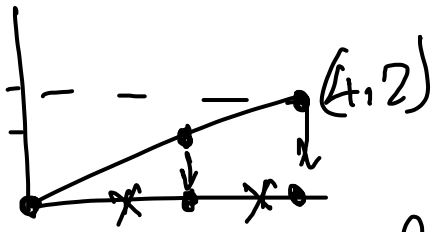
Projection

- Given f_S, $S \subseteq \mathbb{N}^m$



Given f_S, can we compute $f_{S\downarrow\mathbb{N}^n}$ in poly. time?

- eg.



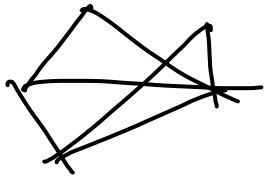
← has gaps (but still got convexity)

- Ans: In general, NO! Moreover, $f_{S\downarrow\mathbb{N}^n}$, written in anyway, could have exponential length.

In other words, computing $f_{S\downarrow\mathbb{N}^n}$ is HARD.

– What does hard mean? Recall

NP-complete : Yes/No output. If Yes, there should be a short (poly. length) verifiable proof.

e.g.  Given G on V of size n. Is G Hamiltonian?

#P Complete : Count all the proofs. ("hardest counting prob")

e.g. Hamiltonian cycle

e.g. $n \in$ Primes (@NP.)

Thm 1 (N-Pak)

Short G.F.'s do not have short projections, i.e., $\exists$ seq. $\{f_n(t_1,t_2)\}$ s.t. $\ell(f_n) =$ poly(n) but $\ell(f_{n,2})$ is not poly. in n, assuming #P-complete prob's are hard (#P $\subsetneq$ FP/poly).

Thm 2

Let $\left\{ \theta_r = \sum_{0 \le x^2 \le 2^r} t^{x^2} \right\}$. Then θ_r cannot be written as short G.F. of length poly(r), but they are projections of

" " " " " , assuming $\#P \subsetneq FP/poly$.

Lemma

Let $\mathcal{L} \subseteq \mathbb{N}$ which is poly time decidable ($\mathcal{L} \in P$), then $\forall r \forall N$, $\exists$ short G.F. $f_r(u, N, z)$ of length poly in r s.t.

$$\sum_{\substack{x \in \mathcal{L} \\ x \le 2^r}} t^x = \left[\frac{1}{(1-t)(1-u)} - f_r(t, u) \right]_{u=1}.$$

f_r is computable in time poly(r).

- Given $(\alpha, \beta, \gamma) \in \mathbb{N}^3$, $\exists ? x : x^2 \equiv \alpha \pmod{\beta}$, $0 \le x \le \gamma$.

  ↳ NP-problem

  ↳ Also NP-complete

If count #x instead, → #P-complete.