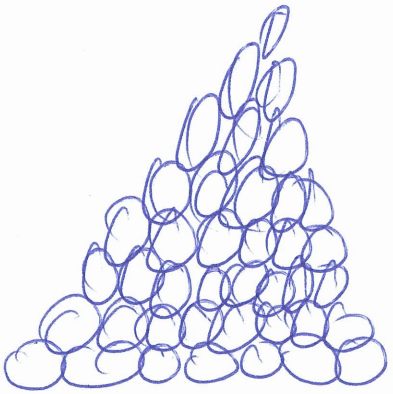
Optimisation by Enumeration

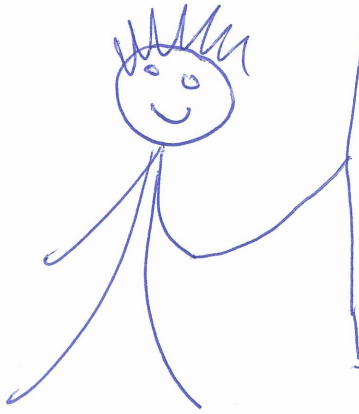
Martin LOEBL, Charles U., Praha

M. L., Discrete Mathematics and Statistical Physics,
Vieweg Advanced Lecture Notes in Math, Nov. 2009

A minicourse Nov 2009, IHP Paris



Give me my biggest stone



I can count the number of biggest stones

Matchings are good!

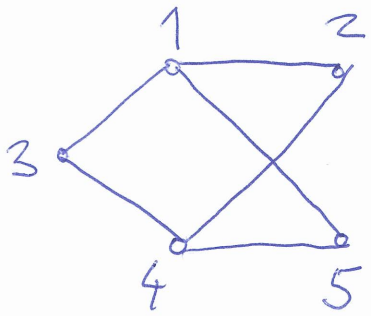
beginning of 60's:

Edmonds: Polynomial-time good characterization
$P \neq NP$

Kac, Ward, Feynman, Kasteleyn, Fisher, Temperley: Combinatorial (2D) statistical physics

$G = (V, E)$ graph

vertices — edges



$M \subseteq E$ matching if $e, e' \in M \Rightarrow e \cap e' = \emptyset$

12, 34 is matching
12, 13 not matching

maximum (weighted) matching

perfect matching

Beginning of Polynomial-time

1963, workshop at the RAND Corp. Jack Edmonds discovered new algorithms to find maximum matching and argued that the algorithm is GOOD i.e. has polynomial complexity.

"For practical purposes the difference between algebraic and exponential order is often more crucial than the difference between finite and non-finite"

The work of Kasteleyn (end of 50's)

$G = (V, E)$ graph, $w : E \to \mathbb{Q}$ weights on edges

Partition fction of dimer arrangements:

$$P(G, x) = \sum_{\substack{E' \subseteq E \\ \text{perfect} \\ \text{matching}}} x^{w(E')}, \text{ where}$$

$$w(E') = \sum_{e \in E'} w(e)$$

↓

• G planar then $P(G, x)$ is a determinant-type expression; may be efficiently calculated.

Do We Understand Complexity Well?

1967 Edmonds conjectures that there is no Pol. algorithm for TSP (i.e. $P \neq NP$)

60's "dimensionality" is crucial in increased complexity of calculating $P(G,x)$. Complexity should grow exponentially with genus of G.

Matching puts together hardness criteria of CS and Stat Phys.

? Is permanent exponentially harder than det ?

Determinantal Complexity

p: real polynomial with variables $x_1, \ldots, x_n$

formula that calculates p: can use $+, \cdot$; start with variables

$L(p)$: size of the least formula for p.

Theorem (Valiant)

If $L(p) = m$ then p is a projection of $\mathrm{Det}_{2m+2}(Y_{i,j})$

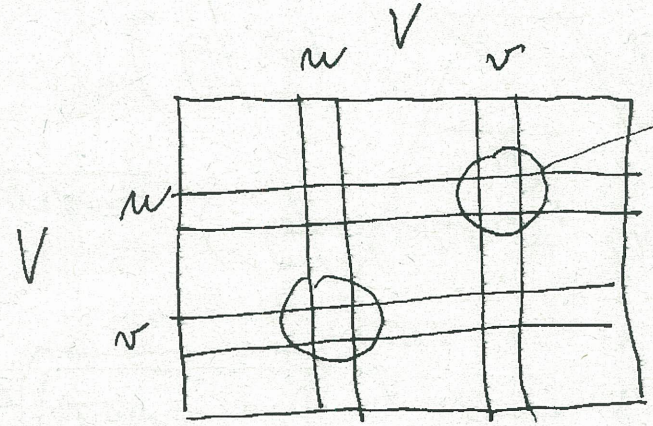
$\to Y_{i,j} := x_\ell$ or a const.

(?) Does permanent (variables $x_{i,j}$) have exponential determinantal complexity (?) Partial results by Mulmuley methods of algebraic geometry

An alternative approach from stat. physics.

$G = (V, E)$ graph D orientation of G

$A(D)$ is $V \times V$ adjacency matrix of D



$$\times^{w(e)} \text{ if } u \xrightarrow{e} v$$

$$-\times^{w(e)} \text{ if } u \xleftarrow{e} v$$

} skew-symmetric

$$\mathrm{Pfaf}(A(D)) = \sum_{\substack{M \text{ perf.} \\ \text{m. of } G}} (-1)^{\#(D,M)} \times^{w(M)}$$

Pfaf is a determinant-type expression

(Gaussian elimination works)

60's: **Kasteleyn** conjectured that: if G has genus g then $P(G,x)$ is a linear combination of 4^g terms of form $\mathrm{Pfaf}(A(D))$, D orientation of G.

Theorem True for planar graphs ($g=0$): $\det$ Pfaf suff.

Theorem [partial res. Regge, Zecchina (96), Galluccio, Loebl (99), Tesler (2000)]

$$P(G,x) = \sum_{i=1}^{4^g} 2^{-g}\, \mathrm{Pfaf}(A(D_i))\,(-1)^{\#_i}$$

for well-defined orientations D_i and numbers $\#_i$.

Cimasoni, Reshetikhin (recently): topological meaning of $\#_i$.

Additive determinantal complexity

Norine (2008, but beginning of 2000's)

G is k-Pfaffian if $P(G,x)$ is linear combination of k terms of form $\mathrm{Pfaf}(A(D))$, D orientation of G, k is smallest possible.

Conjecture (Norine). The Pfaffian number of a graph is always a power of 4.

DISPROVED by Miranda, Lucchesi 09

Theorem (L, Masbaum 09) Conjecture true for Ising partition fction. This is a natural algorithmic process of exponential complexity. Method: combinatorics, statistical physics, geometry

Some byproducts, e.g. G planar iff $Z(G)$ is a "single determinant".

Enumeration char. of planarity

Ising partition fction

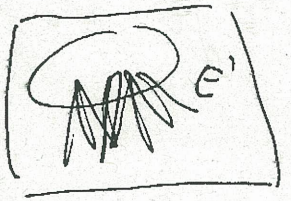
$G = (V, E)$ $\quad \sigma : V \longrightarrow \{1, -1\}$ $\quad$ energy$(\sigma) = -\sum_{e=\{uv\}} w(e)\,\sigma(u)\,\sigma(v)$

$$Z(G, x) = \sum_{\sigma : V \to \{1,-1\}} x^{-\text{energy}(\sigma)}$$

---

generating fction of edge-cuts

$$\mathcal{C}(G, x) = \sum_{\substack{E' \subseteq E \\ \text{edge-cut}}} x^{w(E')}$$



$$Z(G, x) \cdot x^{\sum_E w(e)} = \mathcal{C}(G, x^2)$$

Are these functions rich? (Ising, dimer, Potts ...)

Can they lead to functions which say non-isomorphic graphs apart?

Q-chromatic function [related to Jones polynomial]

$$M_q(G,k) = \sum_{\sigma: V \to \{0,\dots,k-1\} \text{ proper coloring}} q^{\sum \sigma(v)}$$

$$= \sum_{A \subseteq E} (-1)^{|A|} \prod_{W \text{ comp of } (V,A)} (k)_{q^{|W|}}$$

$(k)_q = q^{k-1} + \dots + q + 1$

Example $M_q(K_n,k) = n! \binom{k}{n}_q q^{n(n-1)/2}$

q-dichromate

$$B_q(G,x,y) = \sum_{A \subseteq E} x^{|A|} \prod_{W \in C(A)} (q)_{|W|}$$

Theorem (L, Adv. in math 06)

$$\sum_{A \subseteq E} \prod_{W \in C(A)} (k)_{|W|} \prod_{uv \in A} z_{uv} = \sum_{s : V \to \{0,\dots,k-1\}} q^{\sum_{v \in V} s(v)} e^{\sum_{uv \in E} J_{uv} \Delta(s(u), s(v))}$$

$$z_{uv} = e^{J_{uv}} - 1$$

☺

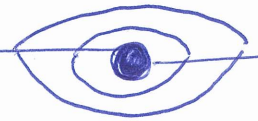
B_q is partition fction of Potts model in magnetic (field)

Conjecture (L, 06).

B_q recognises non-isomorphic chordal graphs.

? Is permanent exponentially harder than determinant (?)

FACT: permanents can be well approximated
- for 0,1 matrices (Jerrum, Sinclair, Vigoda 2000)
- several approximation algorithms for general matrices



This may help us to (efficiently) solve ? ? ? any decision problem in BQP: computable with bounded error in poly-time using quantum resources (e.g. factoring).

Jones polynomial of a link L is defined by skein relation

$$q^2 J\Big($$ $$\Big) - q^{-2} J\Big($$ $$\Big) = (q - q^{-1})\, J\Big($$ $$\Big)$$

$$J(\text{unknot}) = q + q^{-1}.$$

<u>Theorem (L, Moffatt 2009).</u>

$$J(L) =_q \operatorname{per}(M_L)$$

<u>method</u>: R-matrix state sum for J.

Jones and Quantum Computing

Freedman, Kitaev, Larsen, Wang, Aharonov, Jones ...

Theorem ( )

Suppose we have a BQP language and an input x. Then we can construct a link L, of size polynomial in $|x|$, such that

if x is in the language then $\left|J(L, e^{2\pi i/5})\right| < [2]_5^{|x|+1} \cdot 0{,}39$

x not — " — $\left|J(L, e^{2\pi i/5})\right| > [2]_5^{|x|+1} \cdot 0{,}65$

$[2]_5 = 2\cos \pi/5$

These are weak, additive approximations of Jones polynomial [Borodewich, Freedman, Lovász, Welsh]

---

computer experiments initiated with Moffatt, Plechač.

DNA-inspired information concealing

with L. Kencl (2009)

sequence concealing problem: input w, output w_F

I. s segment of w with $|w| \leq k$ $\Rightarrow$ s segment of w_F

II. it is hard to reconstruct w from w_F

III. $|w_F|$ is linear in $|w|$

IV. Relative frequency of segments of w of short length is preserved in w_F

The concealed sequence (output) w_F gives rise to set $S \ni w$ $|S|$ exponential, of feasible reconstructions indistinguish. from information contained in w_F and knowledge of conc. alg.

Repeats in DNA Families of repeating segments (repeats): obstacle in DNA reconstruction by hybridisation

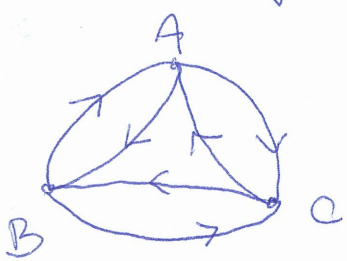
Example. A|B , B|A , A|C , C|A , C|B , B|C

feasible reconstructions:

ABCACB ABCBAC ABACBC

AB
BC
CA
AC
CB
BA

de Bruin graph



econstructions ≡ closed Euler walks

rratia, Bollobás, Coppersmith, Sorkin (2000): Interlace polynomial

Conjecture (Blamey, Kencl, L) (09)
The function of repeats in DNA may be concealing: concealed genetic info of each cell in the form of DNA is available for observations. This helps development of multicellular organisms [the cells are autonomous]