Random Vectors, Random Matrices, and Diagrammatic Fun

Cristopher Moore
University of New Mexico & Santa Fe Institute

joint work with Alexander Russell
University of Connecticut
A product of inner products

• Given $G=(V,E)$ and a complex vector $x_v$ for each $v$, consider the product

$$\prod_{(u,v) \in E} \langle x_u, x_v \rangle$$

• e.g. $\langle x_1, x_2 \rangle \langle x_2, x_3 \rangle \langle x_3, x_1 \rangle |\langle x_3, x_4 \rangle|^2$
Now, with random vectors

• with $x_v$ uniform on the complex $k$-sphere,

$$q(G; k) = \exp \prod_{\{x_v\}} \prod_{(u,v) \in E} \langle x_u, x_v \rangle$$

• what is $q(G; k)$? How hard is it to compute?

• Note: $q(G; k) = 0$ unless $G$ is Eulerian; otherwise rotate $x_v$ by a random phase

$$\langle x, y \rangle = \sum_{i=1}^{k} x_i^* y_i$$
Circuit partitions

- if there are $r_t$ partitions of edges into $t$ cycles, the Circuit Partition Polynomial is

$$j(G; z) = \sum_{t=1}^{\infty} r_t z^t$$

- e.g. $j(G; z) = z + z^2$
- #P-complete under Turing reductions
From integrals to combinatorics

• Theorem:

\[ q(G; k) = \left( \prod_{v \in V} \frac{(k - 1)!}{(k + d_v - 1)!} \right) j(G; k). \]

• Corollary: \( q(G; k) \) is \#P-complete too

• Why this identity?
Outer products and tensors

• Inner product is a contraction of tensors:

\[ q(G; k) = \langle x_1, x_2 \rangle \langle x_2, x_3 \rangle \langle x_3, x_1 \rangle \langle x_3, x_4 \rangle^2 \]

\[ = |x_1\rangle\langle x_1|_{\alpha} |x_2\rangle\langle x_2|_{\beta} |x_3 \otimes x_3\rangle\langle x_3 \otimes x_3|_{\gamma\delta} |x_4\rangle\langle x_4|_{\eta} . \]

• **Einstein convention:** \( \text{tr } M = M_{\alpha}^{\alpha}, \ (UV)^{\alpha}_{\gamma} = U_{\beta}^{\alpha} V_{\gamma}^{\beta} \)
A sum over permutations

\[
\text{Exp}_v |v\rangle \langle v| = \frac{1}{k} \mathbf{1} = \frac{1}{k} \delta_\alpha^\alpha
\]

\[
\text{Exp}_v |v \otimes v\rangle \langle v \otimes v| = \frac{1}{k(k + 1)} \left( \delta_\alpha^\alpha \delta_\beta^\beta + \delta_\beta^\alpha \delta_\alpha^\beta \right)
\]

\[
\text{Exp}_x |x \otimes d\rangle \langle x \otimes d| = \frac{(k - 1)!}{(k + d - 1)!} \sum_{\pi \in S_d} \pi
\]

• Proof: commutes with any \( \pi \) and has trace 1
Wiring the vertices

• Averaging over $x_v$ turns each $v$ into a sum over matchings of incoming and outgoing edges

• Sum of diagrams, each a cycle cover
Tracing the cycles

- Recall the vectors $x_v$ are $k$-dimensional
- For each cycle, $k$ choices of basis vector $v$
- A diagram with $t$ cycles contributes $k^t$, so
  \[ q(G; k) \propto j(G; k) \]
- Real vectors $\Rightarrow$ undirected graphs
- #P-complete?
Determinant and Permanent

- Let $A$ be a $n \times n$ matrix with entries in $\{0, 1\}$

$$\det A = \sum_{\pi \in S_n} (-1)^\pi \prod_i A_{i, \pi_i} \quad \text{perm } A = \sum_{\pi \in S_n} \prod_i A_{i, \pi_i}$$

- $\det A$: geometric meaning, basis-independent, homomorphomorphic, easy

- $\text{perm } A$: combinatorial, basis-dependent, hard
Complexity

- 0-1 PERMANENT is \#P-complete [Valiant ’79]
- However, it can be approximated using a rapidly-mixing Markov chain that samples random perfect matchings [Jerrum, Sinclair, Vigoda ’04]
- Is there another approach, which is purely algebraic?
Godsil-Gutman estimator

• Let $A$ be a $n \times n$ matrix with entries in $\{0, 1\}$

• Let $M_{ij} = \gamma_{ij} A_{ij}$ for uniformly random $\gamma_{ij} \in \{\pm 1\}$

• Then

$$\mathbb{E} \left[ (\det M)^2 \right] = \text{perm } A$$
What?!

- It’s true and, better yet, simple:

\[
\mathbb{E} \left[ (\det M)^2 \right] = \mathbb{E} \sum_{\pi,\sigma} (-1)^{\pi\sigma} \prod_i M_{i,\pi i} M_{i,\sigma i}
\]

- only contributing terms appear when \( \pi = \sigma \) and all \( M_{i,\pi i} \) are nonzero:

\[
= \sum_\pi (-1)^{\pi\pi} \left( \prod_i M_{i,\pi i} \right)^2 = \sum_\pi \prod_i A_{i,\pi i}
\]
But what’s the variance?

- For matrix $A$, define $X = (\det M)^2$. Then
  \[
  \mathbb{E}[X] = \text{perm } A
  \]

- How many samples do we need? Chebyshev:
  \[
  t \approx \frac{\mathbb{E}[X^2]}{\mathbb{E}[X]^2}
  \]

- Can we control this ratio?
Sadly...

- [KKLLL '93]: \[ \frac{\mathbb{E}[X^2]}{\mathbb{E}[X]^2} = 3^{n/2} \cdot \text{poly}(n) \]

- But, they show that if \( \gamma_{ij} \) is uniform on the unit circle, or even just the cube roots of 1,
  \[ \frac{\mathbb{E}[X^2]}{\mathbb{E}[X]^2} = 2^{n/2} \cdot \text{poly}(n) \]

- Can we do better?
Higher-dimensional algebras?

• Barvinok: what if the $\gamma_{ij}$ are quaternions? Or higher-dimensional objects?

• [Chien, Rasmussen, Sinclair ’03]
  In the Clifford algebra of dimension $d$,

  \[
  \left(1 + O\left(\frac{1}{d}\right)\right)^{n/2}
  \]

• In particular, for the quaternions, $\left(\frac{3}{2}\right)^{n/2}$

• Bad news: for $d>2$, we don’t have an algorithm!
How to define the determinant?

• In the nonabelian case, order matters

• The conventional determinant takes each product from top to bottom: no efficient algorithm is known!

• [Barvinok ’00]: symmetrize each term:

  \[
  \text{sdet } M = \frac{1}{n!} \sum_{\pi, \alpha \in S_n} (-1)^\pi \prod_i M_{\alpha_i, \pi \alpha_i}
  \]

• \(O(n^d)\) algorithm in a \(d\)-dimensional algebra
Algebraic estimators

- Define $M_{ij} = \rho_{ij} A_{ij}$, where $\rho_{ij}$ is drawn from some distribution on a nonabelian algebra $A$
- The Haar measure on unitary $d \times d$ matrices
- The Gaussian measure on $d \times d$ matrices (independent entries)
- $\det M$ takes values in $A$
- Define $X = \| \det M \|^2$ or $X = |\text{tr} \det M|^2$
Our results

- Two ways to get a scalar estimator:
  \[ X = |\text{tr} \det M|^2 \quad X_s = |\text{tr} \ \text{sdet} \ M|^2 \]

- We establish the following ratios:
  \[
  \frac{\mathbb{E} [X^2]}{\mathbb{E} [X]^2} = \left( 1 + O\left( \frac{1}{d} \right) \right)^n \quad \frac{\mathbb{E} [X_s^2]}{\mathbb{E} [X_s]^2} = \Omega\left( \frac{2^n}{n^d} \right)
  \]

- Ratios differ by \( O(d^4) \) for \( X = \| \det M \|^2 \)
Permuted products

\[ \mathbb{E}\{\rho_{ij}\}[X_s] = \sum_{\kappa \vdash A} \mathbb{E}\{\sigma_i\} \mathbb{E}_{\alpha,\beta} \left( \text{tr} \prod_i \sigma_{\alpha i} \right) \left( \text{tr} \prod_i \sigma_{\beta i}^* \right) \]

= \quad a_d \cdot \text{perm} \ A

• where

\[ a_d = \mathbb{E}\{\sigma_i\} \mathbb{E}_{\alpha,\beta} \left( \text{tr} \prod_i \sigma_{\alpha i} \right) \left( \text{tr} \prod_i \sigma_{\beta i}^* \right) \]

• Covariance between a product of random matrices \( \sigma_i \) taken in two different orders
The Cupcap Cometh

• What, for instance, is

$$E_{\sigma_1, \sigma_2, \sigma_3} (\text{tr} \, \sigma_1 \sigma_2 \sigma_3) \, (\text{tr} \, \sigma_1 \sigma_3 \sigma_2)^* \ ?$$

• Both Haar and Gauss: $$E[\sigma^i_j (\sigma^k_\ell)^*] = \frac{1}{d} \delta^{ik} \delta_{j\ell}$$

• Diagrammatically:

$$E[\sigma \times \sigma^*] = \frac{1}{d} \bigcup$$
Diagrams and loops

- Form product by “weaving” matrices, and connect with cupcaps
- Tracing gives a factor of $d$ for each loop

\[
E_{\sigma_1,\sigma_2,\sigma_3} \left( \text{tr} \sigma_1 \sigma_2 \sigma_3 \right) \left( \text{tr} \sigma_1 \sigma_3 \sigma_2 \right)^* = \frac{1}{d^2}
\]
A generating function

- Averaging over all permutations gives

\[ a_d = \frac{1}{d^n} \mathbb{E}_\alpha d^c([\alpha, r]) \]

- where \( c(\pi) \) is the number of cycles and \( r = (1 \ 2 \ \cdots \ n) \) is a rotation

- Using Fourier analysis on \( S_n \),

\[ a_d = \frac{1}{d^n} \left( \binom{n + d}{n + 1} - \binom{d}{n + 1} \right) \]
Fourier analysis

• First we write \( a_d = \frac{1}{d^n} \mathbb{E}_{r,r'} d^{c(rr')} \)

• Then \( a_d \) is an inner product \( \langle d^{c(\cdot)}, P \ast P \rangle \)

where \( P \) is the uniform distribution on \( n \)-cycles

• \( d^{c(\cdot)} \) is the trace of a combinatorial representation: action of \( S_n \) on strings of length \( n \) over \( \{1, \ldots, d\} \)

• Fourier coefficients are Kostka numbers

• \( P \) is supported on “hooks”

The k-hook
The second moment

• The fourth moment is a sum of cupcaps:

\[ E_\sigma [\sigma \otimes \sigma \otimes \sigma^* \otimes \sigma^*] = \frac{1}{d^2} \left( \sum \, \text{cupcaps} \right) \]

• Sum over “double covers” in which each \( \rho_{ij} \) appears 0, 2, or 4 times

• More work, but similar ideas
The second moment

- Now the second moment can be bounded in terms of
  \[ E_{\pi, \sigma \in S_{2n}} d^c(\pi^{-1}(r,r)\pi \sigma^{-1}(r,r)\sigma) \]

- Complicated distribution of pairs of \( n \)-cycles in \( S_{2n} \)

- Bound in terms of uniform distribution

- Littlewood-Richardson rule: restrictions of irreps of \( S_{2n} \) to the Young subgroup \( S_n \times S_n \)
Oh, the irony

- We have a family of estimators with ratio $(1+\varepsilon)^n$, but with no efficient algorithm
- We have a family of estimators that we can compute efficiently, but with ratio $\sim 2^n$
- Is there algebraic estimator which is both concentrated and efficiently computable?
Permuted products in finite groups

• If $\sigma$ is an irreducible representation of $G$,

$$\mathbb{E}[\sigma \otimes \sigma^*] = \frac{1}{d} \bigcup$$

• Let $G$ be "highly nonabelian" or "quasirandom": smallest irrep has large $d$

• Then for most permutations $\sigma$ the pair

$$(g_1 g_2 \cdots g_t, g_{\sigma(1)} g_{\sigma(2)} \cdots g_{\sigma(t)})$$

is close to uniform in $G \times G$

• E.g. multiply by $(g, g^{-1})$ — $\sigma$ reverses order
Conclusion

• Where
  • random vectors
  • random matrices
  • random group elements

are concerned, diagrammatic methods can turn averages/integrals into combinatorial problems...

• which can often be solved with Fourier analysis
An advertisement

- A *representation* of a group $G$ is a homomorphism $\psi$ from $G$ to the unitary $d \times d$ matrices...

- But what if there is no such thing? Theorem:

$$\Pr[\psi(xy) = \psi(x)\psi(y)] \leq \frac{1}{2} + \frac{1}{2} \sqrt{\frac{d}{d_{\min}}}$$

- No “low-dimensional embeddings” of $G$!

- Corollary: if $f$ is a function from $G$ to $H$ and most of $H$’s irreps have low dimension,

$$\Pr[f(xy) = f(x)f(y)] \approx \frac{1}{|H|}$$

- No “approximate homomorphisms” from $G$ to $H$
Another advertisement

This book rocks! It's 900+ pages of awesome. It's a book I wish I had written, but now I'm saved the effort. You somehow manage to combine the fun of a popular book with the intellectual heft of a textbook.

— Scott Aaronson

A treasure trove of information on algorithms and complexity, presented in the most delightful way.

— Vijay Vazirani

Oxford University Press, 2011

THE NATURE of COMPUTATION

Cristopher Moore
Stephan Mertens