Computational complexity and 3-manifolds and zombies

Eric G. Samperton

UC Davis

April 9, 2015

Joint work with Greg Kuperberg.
**Table of Contents**

1. Review
2. Complexity & 3-manifolds
3. Proof idea
4. Zombified circuits
5. Applying universality
6. Universality á la Dunfield-Thurston
Goals of complexity theory

- Classify problems based on minimal computational resources needed to solve them.
- Group problems based on similarities (i.e. define complexity classes).
- Understand what it means for one problem to be harder than another (the notion of a reduction).

Leads to interesting questions: what does it mean to be computable, what should be considered fast, etc...
Roughly speaking

- Problems in P are easy to decide.
- For every "YES" instance of a problem in NP, there exists a short proof/witness/certificate of "YES" that is easy to check. All certificates for a given input have a fixed length that is polynomial in the size of the input.
- A problem in \( \#P \) counts the number of accepting proofs of instances of a problem in NP.
- For a problem \( K \), another problem \( L \) is \( K \)-hard if every instance \( x \) of \( K \) can quickly be converted to an instance \( \tilde{x} \) of \( L \) in such a way that

\[
L(\tilde{x}) = 1 \iff K(x) = 1.
\]

- A problem is NP-\textit{complete} if it is NP-hard (\( K \)-hard for every \( K \) in NP) and if it is in NP. Similarly for \( \#P \)-complete and \( \#P \)-hard.
Archetypical examples

Hamiltonian cycle (HAM):

- **Instance**: a finite graph.
- **Decision problem**: Does there exist a loop starting and ending at the same point that traverses each vertex exactly once?

HAM ∈ NP. Proof: Just take proofs to be cycles. It’s easy to check if one is Hamiltonian or not.

Caveat: a proof does not have to be correct, it just has to be easy to decide if it is or not.

In fact, HAM is NP-complete.
Number of Hamiltonian cycles ($\#HAM$):

- **Instance:** a finite graph.
- **Counting problem:** How many Hamiltonian cycles are there?

Corollary: $\#HAM \in \#P$.

Furthermore, the proof that HAM is NP-complete shows $\#HAM$ is $\#P$-complete.

(Note: this does not always have to happen, *i.e.* there exist NP-complete problems without corresponding $\#P$-complete problems.)
Final complexity remarks

- Problems in P are considered tractable.
- $P \subset NP$. I haven't been able to prove it, but probably $P \neq NP$.
- NP-hard and $\#P$-hard problems are conjectured to be intractable, with $\#P$-hard problems qualitatively more intractable than NP-hard problems.
Why are topological 3-manifolds special?

Because they’re computable! That is, the set of topological 3-manifolds is recursively enumerable.

- Moise: every topological 3-dimensional manifold admits a unique PL structure.

Contrast this with higher dimensions:

- Kirby-Siebenmann and Freedman: not true for $n$-manifolds when $n \geq 4$.
- Freedman and Manolescu: even stronger results for $n$-manifolds when $n \geq 4$.

Question: Are topological $n$-manifolds recursively enumerable?
High dimensional manifolds are hopelessly complex

Even without these hard theorems, if one restricts to PL or smooth $n$-manifolds for any fixed $n \geq 4$, basic problems are provably impossible to solve. For example, it’s impossible to decide when two PL 4-manifolds are homeomorphic. On the other hand, it’s a folk theorem that geometrization implies the 3-manifold homeomorphism problem is solvable.

This situation begs the question:
What about the complexity of 3-manifold problems?

Room for exploration. For example:

- Hass-Lagarias-Pippenger: unknotting $\in$ NP.
- Kuperberg: knotting $\in$ NP (modulo GRH!).

Thus, unknotting $\in$ NP $\cap$ coNP. There are no obvious complexity theoretic hypotheses, such as $P \neq NP$, to think there can’t be an efficient algorithm for unknotting.
Quantum algorithms?

Some results in the quantum realm:

- Vertigan, Jaeger-Vertigan-Welsh: \#P-hard to exactly compute the Jones polynomial, except at “lattice roots of unity.”
- Freedman-Larsen-Wang, Freedman-Kitaev-Wang: topological quantum computing, i.e. certain approximations to quantum invariants can be used to build a quantum computer.
- Kuperberg: it seems the types of approximations of quantum invariants that are useful for topology are \#P-hard.

Any applications of quantum computing to algorithms for topology would require novel ideas.
Main Theorem

Fix a finite nonabelian simple group $G$. Let $\mathcal{F}_G$ be the homomorphism counting function

$$\mathcal{F}_G(M) := \# \text{Hom}[\pi_1(M), G]$$

where $M$ is a closed and orientable triangulated 3-dimensional manifold.

Theorem (Kuperberg-S)

The problem of computing $\mathcal{F}_G$ is $\#P$-complete. Relatedly, the problem of deciding for which 3-manifolds $M$ it is true that $\mathcal{F}_G(M) > 1$ is NP-complete.
Heegaard encodings

Instead of triangulated 3-manifolds, we will use Heegaard encodings. For every $g$ fix a standard finite generating set of the mapping class group $\text{Mod}(\Sigma_g)$ of a genus $g$ closed and orientable surface.

A *Heegaard encoding* is a pair $(g, \phi)$ where $\phi$ is a word in the chosen generating set of $\text{Mod}(\Sigma_g)$. The data $(g, \phi)$ encodes the 3-manifold $M$ formed by the Heegaard splitting $H_0 \amalg \phi H_1$, and is polynomially equivalent to a triangulation of $M$. 
Pictures!

Figure: The Humphreys generators.

Figure: A Heegaard splitting.
Van Kampen’s theorem implies that deciding when $F_G > 1$ is in NP, and, hence, computing $F_G$ exactly is in #P:

$$\pi_1(M_\phi) = \langle \alpha_1, \ldots, \alpha_g \mid \alpha_1 = \phi_*(\alpha_1), \ldots, \alpha_g = \phi_*(\alpha_g) \rangle$$

Take certificates as assignment $\alpha_i \mapsto g_i \in G$, and check: (i) one of the $g_i$ is nontrivial and (ii) the assignment is a homomorphism.

The hardness result is the hard part.
Analogy with topological quantum computing

Localizing the action of $\text{Mod}(\Sigma)$ on the set $\{\pi_1(\Sigma) \to G\}$ makes things start to look like reversible computing.

**Figure:** Computational subsurfaces. Homomorphisms $\pi_1(\Sigma^1_C) \to G$ will play the role of logical $G$-dits, whereas the image of an element of $\pi_1$ in $G$ is like a physical $G$-dit.
Planar reversible circuits

Let $A$ be a finite set, called an alphabet. A reversible planar circuit with $n$ inputs over $A$, denoted $C$, is a factorization of an element of $\text{Sym}(A^n)$ as a product of elements of subgroups of the form

$$\{e\} \times \cdots \times \text{Alt}(A \times A \times A) \times \{e\} \times \cdots \times \text{Alt}(A \times A \times A) \times \{e\} \times \cdots \times \{e\}.$$ 

Elements of $\text{Alt}(A \times A \times A)$ are called gates.

This definition is nonstandard, but can be shown to be equivalent to usual definitions, and is more pertinent.
A reversible planar circuit
Simulate reversible circuits with the \( \text{Mod}(\Sigma) \) action on \( \{ \pi_1(\Sigma) \to G \} \).

More carefully, want to formulate a constraint satisfaction problem for reversible circuits that reduces to computing \( \mathcal{F}_G \).
A typical complete problem for reversible circuits

Fixed $A$, and “initialization” and “finalization” subalphabets $I, F \subset A$. Given an $n$-input reversible circuit $C$ over $A$, does there exist a solution pair $C(x) = y$ where $x \in I^n$ and $y \in F^n$? How many such solutions are there?
An imperfect analogy

Three issues to address:

1. Most glaring: the action of $\text{Mod}(\Sigma)$ on $\{\pi_1(\Sigma) \to G\}$ is intransitive. How do we characterize orbits?

2. By our definition, gates are allowed to be arbitrary elements of $\text{Alt}(A^3)$. So we need to find an orbit $\mathcal{O}$ on which the action by $\text{Mod}$ contains all of $\text{Alt}$.

3. Once we’ve found that orbit, we need to ensure that none of the other orbits contribute to $\mathcal{F}_G$. 
The last issue leads us to zombification. The orbit of the trivial homomorphism $\pi_1(\Sigma^1_C) \to G$ threatens to poison the whole simulation.

We stop the epidemic by introducing a new hard problem for reversible circuits, $\text{ZSAT}(A^F_I)$. This problem captures the underlying combinatorics of computing with $\mathcal{F}_G$ in a local way. Some topology, some group theory (including the classification of finite simple groups), and a growth rate argument show that, for appropriate $A, I$ and $F$, $\# \text{ZSAT}(A^F_I)$ reduces to computing $\mathcal{F}_G$. 
Zombified planar circuits

Fix an element $z \in A$, called the zombie digit.

We say a circuit $C$ is *zombified* if every gate stabilizes every $z$ entry. That is, the gates are elements $\sigma$ of the subgroup of $\text{Alt}(A \times A \times A)$ such that for all $a, b \in A$,

$$
\begin{align*}
\sigma(z, a, b) &= \sigma(z, *, *), \\
\sigma(a, z, b) &= \sigma(*, z, *), \\
\sigma(a, b, z) &= \sigma(*, *, z), \\
\sigma(z, z, a) &= \sigma(z, z, *),
\end{align*}
$$

etc. . . .
The problems

Let $I, F \subset A$ be subalphabets, called the initialization and finalization conditions, respectively.

Zombie reversible circuit satisfiability $\text{ZSAT}(A_f^F)$:

- **Instance:** a zombified reversible circuit $C$ with $n$ inputs over $A$.
- **Question:** Does there exist a solution to $C(x) = y$ with

  $$x \in (I \cup \{z\})^n \setminus \{(z, \ldots, z)\}$$

  and

  $$y \in (F \cup \{z\})^n \setminus \{(z, \ldots, z)\}?$$

$\# \text{ZSAT}(A_f^F)$ asks for the number of such solutions.
Zombie completeness

**Proposition**

*With a few basic assumptions on $A$, $I$ and $F$, $ZSAT(A_I^F)$ is NP-complete and $\#ZSAT$ is $\#P$-complete.*
The Mod action is rich

**Theorem (Universality theorem; soft version)**

Let $\Sigma_1^1$ be a genus $g$ surface with one boundary component. For all $g$ large enough, there exists an orbit $O$ of the action of $\text{Mod}(\Sigma_1^g)$ on

$$Y := \left\{ \pi_1(\Sigma_1^g) \to G \right\}/\text{Aut}(G)$$

and a subgroup $\Gamma \leq \text{Mod}(\Sigma_1^g)$ such that the image of $\Gamma$ in $\text{Sym}(Y)$ contains the subgroup

$$\text{Alt}(O) \times \left\{ e_{\text{Sym}(Y\setminus O)} \right\}.$$

We will explain where this comes from below.
Sketch of proof of main theorem

Fix $N$ large enough genus so the universality theorem applies. Consider zombified circuits $C$ with $n$ inputs over the alphabet

$$A := \mathcal{O} \cup \{z = \text{trivial homomorphism}\}.$$  

Fix a genus $Nn$ Heegaard surface $\Sigma_{Nn}$ of $S^3$. As above, localize by identifying $n$ disjoint copies of $\Sigma^1_N$ inside $\Sigma_{Nn}$. Let

$$I := \{[f] \in A \mid f \text{ factors through lower handlebody}\}$$

and

$$F := \{[f] \in A \mid f \text{ factors through upper handlebody}\}.$$  

Check that $\# \text{ZSAT}(A^F_i)$ is $\#P$-complete.
The encoding

For every gate $\sigma \in \text{Aut}(A \times A \times A) \leq \text{Sym}(A^n)$, fix a mapping class $\phi_\sigma \in \text{Mod}(\Sigma_{3N}^1) \leq \text{Mod}(\Sigma_{Nn})$. If $C = \sigma_K \ldots \sigma_1$, let $\phi_C = \phi_{\sigma_K} \ldots \phi_{\sigma_1}$. Remove a tubular neighborhood of $\Sigma_{Nn}$ from $S^3$, and glue the two resulting copies of $\Sigma_{Nn}$ using $\phi_C$ to get a 3-manifold $M_C$. 
The solution count

The number of solutions to $C$ will be

$$\frac{\#\{\pi_1(M_C) \rightarrow G\} - 1}{|\text{Aut}(G)|^k},$$

where $M_C$ is the 3-manifold constructed in linear time from $C$ by replacing gates with appropriate mapping classes. Indeed, just need to check that there are no nontrivial homomorphisms from $\pi_1(M_C) \rightarrow G$ that don’t correspond to solutions of $C$. This follows because our mapping classes that simulate gates leave the orbits away from $O$ pointwise fixed, so nontrivial maps not in $O$ can’t possibly factor through both handlebodies.
Remark on the zombie digit

The pesky adjective “nontrivial” is the whole reason we introduced zombified circuits, since we can’t expect to stop local triviality.
Toward complete orbit invariants

To any homomorphism

\[ f : \pi_1(\Sigma^1_g) \rightarrow G \]

with \( f(\partial) = d \) where

\[ \partial := [a_1, b_1]...[a_g, b_g] \]

is “the” boundary word for \( \pi_1(\Sigma^1_g) \), there is a corresponding map of pairs

\[ f_\# : (\Sigma^1_g, \partial) \rightarrow (BG, d), \]

well defined up to homotopy, where \( BG \) is the classifying space of \( G \) and \( d \) has been identified with a loop in \( BG \).
Pick your poison

From $f_\#$, pass to either one of two equivalent $\text{Mod}(\Sigma^1_g)$ invariants:

- The map induced on relative $H_2$ (which is equivalent to the relative homology class of $f_\#(\Sigma^1_g, \partial)$ in $BG$):

$$f_* : H_2(\Sigma^1_g, \partial \Sigma^1_g) \to H_2(G, d).$$

Note: our coefficients are always $\mathbb{Z}$.

- The relative bordism class of $f_\#$ in $\Omega_2(G, d)$.

In either case, denote the invariant by $[f]$, and call it the Conway-Parker invariant. Recall: $H_2(G, d) \cong \Omega_2(G, d)$ is finite.
A beautiful argument of Livingston, cf. Dunfield-Thurston

**Theorem**

For $i = 1$ and 2, let $f_i : \pi_1(\Sigma_{g_i}^1) \to G$ be a surjection. Then $[f_1] = [f_2]$ if and only if $f_1$ and $f_2$ are stably equivalent.

**Figure:** Stably equivalent $f_1$ and $f_2$. 
Complete, stable orbit invariants for surjections

A little more work shows

**Proposition**

*For all* $g$ *large enough, the Conway-Parker invariant is a complete invariant of the orbits of the action of* $\text{Mod}(\Sigma_g)$ *on*

$$\{f : \pi_1(\Sigma_g) \to G \mid f \text{ is surjective}\}.$$  

*There is a similar statement for the action of* $\text{Mod}(\Sigma_g)$ *on*

$$\{f : \pi_1(\Sigma_g) \to G \mid f \text{ is surjective}\}/\text{Aut}(G).$$
What about simplicity of $G$?

**Lemma (Hall’s Lemma)**

Suppose $G_1, \ldots, G_k$ are nonabelian finite simple groups and let $F_g$ be the free group on $g$ generators. For all $i$ let $f_i : F_g \to G_i$ be a surjection. If for all $i$ and $j$, there is no isomorphism $\alpha_{ij}$ such that $f_i = \alpha_{ij} \circ f_j$, then the product map

$$f_1 \times \cdots \times f_k : F_g \to G_1 \times \cdots \times G_k$$

is surjective.
Put it together

Combining Hall’s lemma and the stable orbit description with a little homological algebra:

**Theorem**

Let $G$ be nonabelian simple. Fix an integer $k$. Then for all $g$ large enough, $\text{Mod}(\Sigma_g^1)$ acts on every orbit in

$$\{ f : \pi_1(\Sigma_g^1) \to G \mid f \text{ is surjective} \}/ \text{Aut}(G)$$

$k$-transitively. Moreover, if $\mathcal{O}_1, \ldots, \mathcal{O}_N$ are the orbits, then $\text{Mod}(\Sigma_g^1)$ acts transitively on

$$\mathcal{O}_1 \times \cdots \times \mathcal{O}_N.$$
By the Classification of Finite Simple Groups...

If a group $A$ acts 6-transitively on a finite set $S$, then the image of $A$ inside $S$ contains $\text{Alt}(S)$.

**Corollary (Surjective universality)**

For all $g$ large enough, the image of $\text{Mod}(\Sigma_g)^1$ in

$$\text{Sym} \left[ \{ f : \pi_1(\Sigma_g^1) \to G \mid f \text{ is surjective} \} / \text{Aut}(G) \right]$$

contains

$$\text{Alt}(\mathcal{O}_1) \times \cdots \times \text{Alt}(\mathcal{O}_N).$$

Remark: Everything in this section up to this point closely follows the work of Dunfield and Thurston in “Finite covers of random 3-manifolds,” Invent. Math., 2006.
Final hurdle: non-surjections

We combine a variant of Hall’s lemma with a rate of growth computation.

**Lemma**

Let $G_1, G_2, \ldots, G_k$ be groups with $G_1$ simple. Suppose $G_1$ is not involved with $G_i$ for any $i = 2, \ldots, k$. For a subgroup $H$ of $G_1 \times \cdots \times G_k$, let $\pi_i(H)$ denote the projection of $H$ to $G_i$. Then if $\pi_1(H) = G_1$, $H$ contains $G_1 \times \{1\} \times \cdots \times \{1\}$. 
A rate of growth argument

Let

\[ \mathcal{O}_g = \{ f : \pi_1(\Sigma^1_g) \to G \mid f \text{ is surjective and } [f] = 0 \} / \text{Aut}(G). \]

For all \( g \) large enough, surjective universality implies there exists a subgroup \( \Gamma_g \leq \text{Mod}(\Sigma^1_g) \) such that \( \Gamma_g \) is contained in

\[ \text{Alt}(\mathcal{O}_g) \times \text{Sym} \left[ \{ f \mid f \text{ is NOT surjective} \} / \text{Aut}(G) \right]. \]

**Theorem (Universality theorem)**

*For all \( g \) large enough, there is a subgroup \( \Gamma \leq \text{Mod}(\Sigma^1_g) \) such that the image of \( \Gamma \) in \( \text{Sym}[\{ \pi_1(\Sigma^1_g) \to G \} / \text{Aut}(G)] \) contains \( \text{Alt}(\mathcal{O}_g) \).*
Further directions

- Non-simple $G$? Is there a solvable/unsolvable dichotomy?
- Geometric restrictions? E.g., can we restrict our 3-manifolds to be homology spheres?
- Knots and links? I am currently working this out; hardness results should be similar. Universality uses a classifying space for branched covers.
- Other quantum invariants?
- Average case complexity?
Thank you for listening!

Questions?