Counting Homomorphisms Modulo Primes

Andrei A. Bulatov
Simon Fraser University

Joint work with Amirhosein Kazeminia

Ulam, 2021

Counting CSPs

Counting CSP: Given relational structure G and H, find the number of homomorphisms from G to H

$\#CSP(H)$ if H is fixed

$\#CSP(H)$ belongs to the class $\#P$

When every tuple from H is assigned weight, every homomorphism is assigned a weight

$WCSP(H)$ is the problem of finding the total weight of all homomorphisms

Counting Graph Homomorphisms

Theorem (Dyer, Greenhill, 2000)
$\#CSP(H)$, H is a graph, is poly time if and only if every connected component of H is a complete reflexive graph or a complete bipartite graph.
Otherwise $\#CSP(H)$ is $\#P$-complete

The hardness is from the N-graph

It is also a obstruction to a Mal'tsev polymorphism

Linear Equations

$\#CSP(H_{aff})$, where the relations of H_{aff} are given by systems of linear equations over $GF(q)$, is poly time:

- Every instance is a system of linear equations
- Find the dimensionality k of the solution space
- The number of homomorphisms/solutions is q^k

General Counting CSP

Theorem **(**B., 2008, Dyer,Richerby, 2010**)**
$\#CSP(H)$, H is a relational structure, is poly time if and only if for every pp-interpretable equivalence relations α, β the rank $rank(M(\alpha,\beta))$ equals the number of $\alpha \vee \beta$-blocks.
Otherwise $\#CSP(H)$ is $\#P$-complete

$M(\alpha,\beta)$:

Beyond Just Counting

Weighted #CSP:

- rational nonnegative weights, B. et al, 2009
- real and complex weights, Cai,Chen, 2012

Holant: multiple results by Cai and coauthors

Approximation:

- Boolean (partial for weighted), Dyer et al, 2010, B. et al, 2012
- conservative (partial), Chen et al, 2013
- graphs (partial), Galanis et al, 2015

Modular Counting

Counting CSP mod p: Given relational structure G and H, find the number of homomorphisms from G to H modulo p, p prime

$\#_p CSP(H)$ if H is fixed

$\#_p CSP(H)$ belongs to the class $\#_p P$

Counting and Automorphisms

Counting 3-colorings mod 3

Counting and Fixed Points

Homomorphisms to a 3-star mod 3

$\#_p CSP(H)$ is poly time equivalent to $\#_p CSP(H^\pi)$ where H^π is the subgraph/substructure induced by the fixed points of automorphism π of order p

Repeating this we eventually obtain that $\#_p CSP(H)$ is poly time equivalent to $\#_p CSP(H^\dagger)$, where $H^\dagger$ has no p-automorphisms

Conjectures and Results

Conjecture (Faben, Jerrum, 2015)

If graph H does not have p-automorphisms, then $\#_p CSP(H)$ is hard whenever $\#CSP(H)$ is hard.

Theorem

$\#_p CSP(H)$, H is a graph, is poly time if and only if every connected component of $H^\dagger$ is a complete reflexive graph or a complete bipartite graph.

Otherwise $\#_p CSP(H)$ is $\#_p P$-complete

What We Know

- trees mod 2	Faben,Jerrum, 2015
- cactus graphs mod 2	Göbel et al, 2014
- square-free mod 2	Göbel et al, 2016
- K_4-minor free	Focke et al, 2021
- trees mod p	Göbel et al, 2018
- square-free mod p	B., Kazeminia, 2019
- $K_{3,3}$ and domino free mod p	Lagodzinski et al., 2020

Algebra for Modular Counting

The main steps of the algebraic approach go through, although with interesting twists

- adding constants
- conjunctions
- quantification
- pp-interpretations

Adding Constants

For a relational structure H let H^c denote the expansion of H with all the constant

Theorem

If H has no p-automorphisms, $\#_p CSP(H^c)$ is poly time reducible to $\#_p CSP(H)$

Proved in Faben/Jerrum 2015 for graphs (through quantum graphs)

In the general case can be done through interpolation as in B./Dalmau 2003

PP-Definitions

If R is a conjunction of predicates of H, then it is straightforward that $\#_p CSP(H + \{R\})$ is poly time reducible to $\#_p CSP(H)$

Quantification is trickier

PP-Definitions II

$\exists^p x$ stands for `there exists $\not\equiv 0 \pmod p$ values of x

$Q(x_1, \dots, x_k) = \exists^p y\ R(x_1, \dots, x_k, y)$ is defined in a natural way

Theorem

If $Q(x_1, \dots, x_k) = \exists^p y\ R(x_1, \dots, x_k, y)$ where R is a predicate of H, then $\#_p CSP(H + \{Q\})$, is poly time reducible to $\#_p CSP(H)$

Proved through old tricks and interpolation

PP-Definitions III

However, we need regular quantification

Theorem

If $Q(x_1, \dots, x_k) = \exists y\, R(x_1, \dots, x_k, y)$ where R is a predicate of H and H has no p-automorphisms, then $\#_p CSP(H + \{Q\})$, is poly time reducible to $\#_p CSP(H)$

Proof idea

Möbius Inversion

Lemma

If $\hom(G_1, H) \equiv \hom(G_2, H) (\mathrm{mod}\ p)$ for any G_1, G_2 then H has a p-automorphism.

Consider $\hom(H, H)$. Let $Part(H)$ be the set of all partitions of $V(H)$

Möbius inversion $inj(H, H) = \sum_{\theta \in Part(H)} \omega_\theta \hom(H/\theta, H)$,

where $\omega_= = 1$ and $\omega_\theta = -\sum_{\eta < \theta} \omega_\eta$

Since $\sum_{\theta \in Part(H)} \omega_\theta = 0$ and $\hom(H/\theta, H) \equiv N (\mathrm{mod}\ p)$,

$$|Aut(H)| = inj(H, H) = \sum_{\theta \in Part(H)} \omega_\theta \hom(H/\theta, H)$$

$$\equiv N \cdot \sum_{\theta \in Part(H)} \omega_\theta \equiv 0 (\mathrm{mod}\ p)$$

PP-Interpretations

Theorem

If H' is pp-interpretable in H and H has no p-automorphisms then $\#_p CSP(H')$ is poly time reducible to $\#_p CSP(H)$

Interpolation + Möbius inversion

Non-Bipartite Graphs

Any 2-element structure can be pp-interpreted in H^c, where H is a nontrivial nonbipartite graph (B. 2005)

Therefore, Faben/Jerrum conjecture holds for nonbipartite graphs.
More generally

Theorem
If H is a relational structure such that it has no p-automorphisms and $CSP(H)$ is NPC then $\#_p CSP(H)$ is $\#_p$-hard

Bipartite Graphs: #BIS

$\#BIS$ ($\#_p BIS$) counting the number of independent sets in a bipartite graph (modulo p)

$\#BIS$ ($\#_p BIS$) is equivalent to $\#CSP(H_N)$ ($\#_p CSP(H_N)$)

$\#BIS(\alpha,\beta)$: $\sum_{I\in IS} \alpha^{|I\cap U|} \cdot \beta^{|I\cap D|}$

There is a problem with $\#_p BIS$

N-Graphs and PP-Definitions

Observation:

If H is a nontrivial bipartite graph then some N-graph is pp-definable in H^c

If $|A|, |B|, |C|, |D| \not\equiv 0 (\mathrm{mod}\ p)$, we are done, as some weighted $\#_p BIS$ is reducible to $\#_p CSP(H)$

Otherwise we have a problem

Homomorphism Vectors

Gx denotes graph G with a distinguished vertex x

$\hom(Gx, Hv)$ is the number of homs φ such that $\varphi(x) = v$

$\hom(Gx, HW) = \sum_{v \in W} \hom(Gx, Hv)$

Lemma

There is Gx such that $\hom(Gx, HA), \hom(Gx, HC) \not\equiv 0 (\mathrm{mod}\ p)$

Homomorphism Vectors II

With a gadget Gx like this we can reduce weighted $\#_p BIS$

Homomorphism Vectors III

We only look at A. There are 3 cases.

Case 1. There is Gx such that $\hom(Gx, Hv_1) \equiv 0$, $\hom(Gx, Hv_2) \not\equiv 0 (mod\ p)$

Then we can manufacture a smaller N-graph

Case 2. $\hom(Gx, Hv_1) \equiv \hom(Gx, Hv_2) \pmod p$ for all Gx, $v_1, v_2 \in A$

Then H has a p-automorphism

Homomorphism Vectors IV

Case 3. There is Gx such that $\hom(Gx, Hv_1) \not\equiv \hom(Gx, Hv_2)\ (mod\ p)$ for some $v_1, v_2 \in A$

Gx induces an equivalence relation on A: $v_1 \sim v_2$ iff $\hom(Gx, Hv_1) \equiv \hom(Gx, Hv_2)\ (mod\ p)$

Let $L_1, \ldots, L_s$ be the corresponding partition

Then either $\hom(G^{(i)}x, HA) \not\equiv 0 (\mathrm{mod}\ p)$, or $|L_j| \equiv 0 (\mathrm{mod}\ p)$

Homomorphism Vectors V

Let $s = 2$, L_1, L_2, and a_1, a_2 the corresponding numbers $\hom(Gx, Hv)$
Then

$$\hom(Gx, HA) \equiv a_1|L_1| + a_2|L_2|$$

$$\hom\left(G^{(2)}x, HA\right) \equiv a_1^2|L_1| + a_2^2|L_2|$$

If both equal 0 then $|L_1| \equiv |L_2| \equiv 0 (\mathrm{mod}\, p)$

Finally, if $|L_1| \equiv \cdots \equiv |L_s| \equiv 0 (\mathrm{mod}\, p)$ for all Gx, then H has a p-automorphism

Thank You!