Fixed-Point Approximations of Graph Isomorphism.

Anuj Dawar
University of Cambridge

FICS, 1 September 2013

joint work with Bjarki Holm
Graph Isomorphism

*Graph Isomorphism:* Given graphs $G, H$, decide whether $G \cong H$ is

- not known to be in PTime
- not expected to be NP-complete.

In practice and *on average*, graph isomorphism is efficiently decidable.
Tractable Approximations of Isomorphism

A tractable approximation of graph isomorphism is a polynomial-time decidable equivalence \( \equiv \) on graphs such that:

\[
G \cong H \quad \Rightarrow \quad G \equiv H.
\]

Practical algorithms for testing graph isomorphism typically decide such an approximation.

If this fails to distinguish a pair of graphs \( G \) and \( H \), more discriminating tests are deployed.
Vertex Classification

The following problem is easily seen to be computationally equivalent to graph isomorphism:

Given a graph $G$ and a pair of vertices $u$ and $v$, decide if there is an automorphism of $G$ that takes $u$ to $v$.

The algorithms we study aim to decide equivalence relations on vertices (or tuples of vertices) that approximate the orbits of the automorphism group.

For such an equivalence relation $\equiv$, we also write $G \equiv H$ to indicate that $G$ and $H$ are not distinguished by the corresponding isomorphism test.

For connected graphs, this means that for every $u$ in $G$, there is a $v$ in $H$ so that $u \equiv v$ in the disjoint union of $G$ and $H$. 
Equitable Partitions

An equivalence relation $\equiv$ on the vertices of a graph $G = (V, E)$ induces an equitable partition if

for all $u, v \in V$ and each $\equiv$-equivalence class $S$,

$$|\{w \in S \mid (u, w) \in E\}| = |\{w \in S \mid (v, w) \in E\}|$$

The naive vertex classification algorithm finds the coarsest equitable partition of the vertices of $G$. 
Colour Refinement

Define, on a graph $G = (V, E)$, a series of equivalence relations:

$$\equiv_0 \supseteq \equiv_1 \supseteq \cdots \supseteq \equiv_i \cdots$$

where $u \equiv_{i+1} v$ if they have the same number of neighbours in each $\equiv_i$-equivalence class.

This converges to the coarsest equitable partition of $G$.

Equivalently, define an operator on the space of equivalence relations on $V$, that takes a relation $\equiv$ to $\equiv'$ defined by letting $u \equiv' v$ if they have the same number of neighbours in each $\equiv$-equivalence class.

The coarsest equitable partition is the greatest fixed point of this operator.
Almost All Graphs

*Naive vertex classification* provides a simple test for isomorphism that works on almost all graphs:

For graphs $G$ on $n$ vertices with vertices $u$ and $v$, the probability that $u \sim v$ goes to 0 as $n \to \infty$.

But the test fails miserably on *regular graphs.*
Weisfeiler-Lehman Algorithms

The $k$-dimensional Weisfeiler-Lehman test for isomorphism (as described by Babai), generalises naive vertex classification to $k$-tuples.

For a graph $G$, let $\equiv^{WL^k}$ be the coarsest equivalence relation on $k$-tuples of vertices so that for $k$-tuples $u$ and $v$, if $u \equiv^{WL^k} v$, then:

- $u$ and $v$ induce isomorphic subgraphs

and for each $k$-tuple $\alpha_1, \ldots, \alpha_k$ of $\equiv^{WL^k}$-classes,

$$|\{u \mid \bigwedge_j u[u/u_j] \in \alpha_j\}| = |\{v \mid \bigwedge_j v[v/v_j] \in \alpha_j\}|$$
Induced Partitions

In other words,

Given an equivalence relation \( \equiv \) on \( V^k \), each \( k \)-tuple \( u \) induces a labelled partition of \( V \).

The labels of the partition are \( k \)-tuples \( \alpha_1, \ldots, \alpha_k \) of \( \equiv \)-equivalence classes, and the corresponding part is the set:

\[
\{ u \mid \bigwedge_j u[u/u_j] \in \alpha_j \}.
\]

Define \( \equiv \) to be the equivalence relation where \( u \equiv' v \) if, in the partitions they induce, the corresponding parts have the same cardinality.

Then, \( \equiv^{WL^k} \) is the greatest fixed point of the operator that takes \( \equiv \) to \( \equiv' \).
Weisfeiler-Lehman Algorithms

If $G, H$ are $n$-vertex graphs and $k < n$, we have:

$$G \cong H \iff G \cong^{WL^n} H \implies G \cong^{WL^{k+1}} H \implies G \cong^{WL^k} H.$$

$G \cong^{WL^k} H$ is decidable in time $n^{O(k)}$.

The equivalence relations $\cong^{WL^k}$ form a family of tractable approximations of graph isomorphism.

There is no fixed $k$ for which $\cong^{WL^k}$ coincides with isomorphism.

Restricted Graph Classes

For many specific graph classes, there is a fixed value of $k$ such that $\equiv_W^L$ coincides with isomorphism:

- trees; planar graphs; graphs of tree-width at most $t$;
- and most generally, graphs that exclude a $t$-clique minor

(Grohe 2010)

The construction of Cai, Fürer and Immerman shows that there is no such $k$ for graphs of

- maximum degree 3; and
- colour class size 4.

Each of these restrictions gives a class with a polynomial-time isomorphism test by other means.
Fixed-Point Logic with Counting

The result of *Cai, Fürer and Immerman* came in the context of proving that there are polynomial-time properties of graphs that are not definable in *fixed-point logic with counting* (FPC).

This is the logic formed by adding to *first-order logic* operators for *least-fixed points* of definable operators as well as *counting terms*

\[
[lfp_{R,x}\varphi](t)
\]

is a formula denoting that the tuple \( t \) is in the least fixed point of the operator defined by \( \varphi \).

If \( \varphi(x) \) is a formula with free variable \( x \), then \( \nu = \#x\varphi \) denotes that \( \nu \) is the number of elements of \( A \) that satisfy the formula \( \varphi \).
**Counting Logic**

$C^k$ is the logic obtained from *first-order logic* by allowing:

- *counting quantifiers*: $\exists^i x \varphi$; and
- only the variables $x_1, \ldots, x_k$.

Every formula of $C^k$ is equivalent to a formula of first-order logic, albeit one with more variables.

We write $G \equiv^{C^k} H$ to denote that no sentence of $C^k$ distinguishes $G$ from $H$.

It is not difficult to show that $G \equiv^{C^{k+1}} H$ if, and only if, $G \equiv^{WL^k} H$. 
Counting Tuples of Elements

Consider extending the counting logic with quantifiers that count *tuples* of elements.

This does not add further expressive power.

\[ \exists^i x y \varphi \]

is equivalent to

\[ \bigvee_{f \in F} \bigwedge_{j \in \text{dom}(f)} \exists^f(j) x \exists^j y \varphi \]

where \( F \) is the set of finite partial functions \( f \) on \( \mathbb{N} \) such that

\[ \left( \sum_{j \in \text{dom}(f)} j f(j) \right) = i. \]

In other words, in the characterisation of \( \equiv^{WL^k} \) in terms of induced partitions, there is no gain in considering partitions of \( V^m \) instead of \( V \).
Infinite Hierarchy

(Cai, Fürer, Immerman, 1992) show that there are polynomial-time decidable properties of graphs that are not definable in fixed-point logic with counting.

For each formula $\varphi$ of $\text{FPC}$ there is a $k$ such that if $G \equiv_{C^k} H$, then $G \models \varphi$ if, and only if, $H \models \varphi$.

They construct a sequence of pairs of graphs $G_k, H_k$ ($k \in \omega$) such that:

- $G_k \equiv_{C^k} H_k$ for all $k$.
- There is a polynomial time decidable class of graphs that includes all $G_k$ and excludes all $H_k$.

Moreover, $G_k, H_k$ can be chosen to be 3-regular and of colour-class size 4.
Given any graph $G$, we can define a graph $X_G$ by replacing every edge with a pair of edges, and every vertex with a gadget. The picture shows the gadget for a vertex $v$ that is adjacent in $G$ to vertices $w_1, w_2$ and $w_3$. The vertex $v^S$ is adjacent to $a_{vw_i} (i \in S)$ and $b_{vw_i} (i \notin S)$ and there is one vertex for all even size $S$. The graph $\tilde{X}_G$ is like $X_G$ except that at one vertex $v$, we include $V^S$ for odd size $S$. 
Properties

If $G$ is connected and has treewidth at least $k$, then:

1. $X_G \not\sim \tilde{X}_G$; and

2. $X_G \equiv ^{C^k} \tilde{X}_G$.

(2) is proved by a game argument, combining cops and robber games on $G$ with a bijection game on $X_G$ and $\tilde{X}_G$.

The original proof of (Cai, Fürer, Immerman) relied on the existence of balanced separators in $G$. The characterisation in terms of treewidth is from (D., Richerby 07).
Rank Logics

The Cai-Fürer-Immerman construction can be reduced to the solvability of systems of equations over a 2-element field.

This motivates an extension of first-order logic with operators for the rank of a matrix over a finite field. (D., Grohe, Holm, Laubner, 2009)

For each prime $p$ and each arity $m$, we have an operator $rk^p_m$ which binds $2m$ variables and defines the rank (over $\mathbb{GF}(p)$) of the $n^m \times n^m$ matrix defined by a formula $\varphi(x, y)$. 

Anuj Dawar

September 2013
Equivalences and Rank Logic

The definition of rank logics yields a family of approximations of isomorphism.

\[ G \equiv_{R, k, \Omega, m}^H \] if \( G \) and \( H \) are not distinguished by any formula of \( \text{FO}(rk) \) with at most \( k \) variables using operators \( rk_p^m \) for \( p \) in the finite set of primes \( \Omega \).

We do not know if these relations are tractable.

But, we can refine them further to obtain a tractable family: \( \equiv_{IM, k, \Omega, m} \).

(D., Holm 2012)
Induced Partitions

For simplicity, consider the case when $m = 1$ and $\Omega = \{p\}$.

Given an equivalence relation $\equiv$ on $V^k$, each $k$-tuple $u$ induces a labelled partition of $V \times V$.

The labels of the partition are $\binom{k}{2}$-tuples $\alpha_1, \ldots, \alpha_l$ of $\equiv$-equivalence classes, and the corresponding part is the set:

$$\{(a, b) \mid \bigwedge_{1 \leq i < j \leq k} u[a/\alpha_i, b/\alpha_j] \in \alpha_{\{i,j\}}\}.$$
Induced Partitions

Let $P^u_1, \ldots, P^u_s$ be the parts of this partition (seen as 0-1 $V \times V$ matrices) and $P^v_1, \ldots, P^v_s$ be the corresponding parts for a tuple $v$.

Let $u \equiv' v$ if, $u \equiv v$ and for any function $\mu : \{1, \ldots, s\} \rightarrow \{0, \ldots, p-1\}$, we have

$$\text{rk}\left( \sum_i \mu(i) P^u_i \right) = \text{rk}\left( \sum_i \mu(i) P^v_i \right).$$

where the rank is in the field $\mathbf{GF}(p)$.

$\equiv^R_{k,\{p\},1}$ is the greatest fixed point of the operator taking $\equiv$ to $\equiv'$.

For general $m$ and $\Omega$, we need to consider partitions of $V^m \times V^m$ and rank and linear combinations over $\mathbf{GF}(p)$ for all $p \in \Omega$. 

Anuj Dawar
September 2013
Invertible Map Equivalence

The relation $\equiv^{IM}_{k,\{p\},1}$ is defined as the greatest fixed point of the operator $\equiv \mapsto \equiv'$ where:

$u \equiv' v$ if $u \equiv v$ and there is an invertible linear map $S$ on the vector space $\mathbf{GF}(p)^V$ such that we have for all $i$

$$SP_i u S^{-1} = P_i v.$$

This implies, in particular, that all linear combinations have the same rank.

A result of (Chistov, Karpinsky, Ivanyov 1997) guarantees that simultaneous similarity of a collection of matrices is decidable in polynomial time to get a family of polynomial-time equivalence relations $\equiv^{IM}_{k,\Omega,m}$. 
Coherent Algebras

Weisfeiler and Lehman presented their algorithm in terms of cellular algebras.

These are algebras of matrices on the complex numbers defined in terms of Schur multiplication:

\[(A \circ B)(i, j) = A(i, j)B(i, j)\]

They are also called coherent configurations in the work of Higman.

**Definition:**
A coherent algebra with index set \( V \) is an algebra \( \mathcal{A} \) of \( V \times V \) matrices over \( \mathbb{C} \) that is:

- closed under Hermitian adjoints;
- closed under Schur multiplication;
- contains the identity \( I \) and the all 1's matrix \( J \).
Coherent Algebras

One can show that a coherent algebra has a *unique basis* $A_1, \ldots, A_m$ (i.e. every matrix in the algebra can be expressed as a linear combination of these) of 0-1 matrices which is closed under *adjoints* and such that

$$\sum_i A_i = J.$$

One can also derive *structure constants* $p_{i,j}^k$ such that

$$A_i A_j = \sum_k p_{i,j}^k A_k.$$

Associate with any graph $G$, its *coherent invariant*, defined as the smallest coherent algebra $A_G$ containing the adjacency matrix of $G$. 
Weisfeiler-Lehman method

Say that two graphs $G_1$ and $G_2$ are WL-equivalent if there is an isomorphism between their coherent invariants $\mathcal{A}_{G_1}$ and $\mathcal{A}_{G_2}$.

$G_1$ and $G_2$ are WL-equivalent if, and only if, $G_1 \equiv C^3 G_2$.

Friedland (1989) has shown that two coherent algebras with standard bases $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ are isomorphic if, and only if, there is an invertible matrix $S$ such that

$$SA_iS^{-1} = B_i$$

for all $1 \leq i \leq m$. 
Complex Invertible Map Equivalence

Define $\equiv^{\text{IM}}_{\mathbb{C},k}$ as the greatest fixed point of the operator $\equiv \mapsto \equiv'$ where:

$\mathbf{u} \equiv' \mathbf{v}$ if there is an invertible linear map $S$ on the vector space $\mathbb{C}^V$ such that we have for all $i$

$$SP_i^u S^{-1} = P_i^v.$$

We can show $\equiv^{\text{IM}}_{\mathbb{C},k+1} \subseteq \equiv^{C}_k \subseteq \equiv^{\text{IM}}_{\mathbb{C},k-1}$. 
Research Directions

We can show that \( \equiv_{4,\{2\},1}^{\text{IM}} \) is the same as isomorphism on graphs of \textit{colour class size} 4.

- For all \( t \), are there fixed \( k, \Omega \) and \( m \) such that \( \equiv_{k,\Omega,m}^{\text{IM}} \) is isomorphism on graphs of colour class size \( t \)?

- What about graphs of degree at most 3? or \( t \)?

Is the \textit{arity hierarchy} really strict on graphs? Could it be that \( \equiv_{k,\Omega,m}^{\text{IM}} \) is subsumed by \( \equiv_{k',\Omega,1}^{\text{IM}} \) for sufficiently large \( k' \)?

Show that no fixed \( \equiv_{k,\Omega,m}^{\text{IM}} \) is the same as isomorphism on graphs.

Note: we can show that \( \equiv_{k,\Omega,1}^{\text{IM}} \) is not the same as isomorphism for any fixed \( k \) and \( \Omega \).
Summary

The Weisfeiler-Lehman family of approximations of graph isomorphism have a number of equivalent characterisations in terms of:

- complex algebras;
- combinatorics;
- counting logics;
- bijection games;
- linear programming relaxations of isomorphism.

We have introduced a new and stronger family of approximations of graph isomorphism based on algebras over finite fields, and these

There remain many questions about the strength of these approximations and their relations to logical definability.