The Graph Isomorphism Problem and the Module Isomorphism Problem

Harm Derksen
Department of Mathematics
Michigan Center for Integrative Research in Critical Care
University of Michigan

Partially supported by NSF DMS 1601229

Symmetry vs Regularity
Pilsen, July, 2018

Publications results for "Author=(derksen, *) AND Title=(graph)"

MR3101711 Reviewed

Derksen, Harm(1-MI)
Department of Mathematics, University of Michigan
Ann Arbor, Michigan, 48109

The graph isomorphism problem and approximate categories. (English summary)

J. Symbolic Comput. 59 (2013), 81–112.
05C60 (20G05 68Q25)

Summary: "It is unknown whether two graphs can be tested for isomorphism in polynomial time. A classical approach to the Graph Isomorphism Problem is the d-dimensional Weisfeiler-Lehman algorithm. The d-dimensional WL-algorithm can distinguish many pairs of graphs, but the pairs of non-isomorphic graphs constructed by Cai, Fürer and Immerman it cannot distinguish. If d is fixed, then the WL-algorithm runs in polynomial time. We will formulate the Graph Isomorphism Problem as an Orbit Problem: Given a representation V of an algebraic group G and two elements $v_1, v_2 \in V$, decide whether v_1 and v_2 lie in the same G-orbit. Then

Orbit Problems

Orbit Problem

G group acting on k-vector space V
given $v, v' \in V$, does there exist $g \in G$ with $g \cdot v = v'$?

Orbit Problems

Orbit Problem

G group acting on k-vector space V
given $v, v' \in V$, does there exist $g \in G$ with $g \cdot v = v'$?

Graph Isomorphism Problem (Hard)

Γ, Γ' graphs with n vertices, $A, A' \in \mathrm{Mat}_{n,n}$ adjacency matrices
$G = \{\text{permutation matrices}\}$ acts on $\mathrm{Mat}_{n,n}$ by conjugation
does there exists a permutation matrix P with $PAP^{-1} = A'$?

Orbit Problems

Orbit Problem

G group acting on k-vector space V
given $v, v' \in V$, does there exist $g \in G$ with $g \cdot v = v'$?

Graph Isomorphism Problem (Hard)

Γ, Γ' graphs with n vertices, $A, A' \in \mathrm{Mat}_{n,n}$ adjacency matrices
$G = \{\text{permutation matrices}\}$ acts on $\mathrm{Mat}_{n,n}$ by conjugation

does there exists a permutation matrix P with $PAP^{-1} = A'$?

Module Isomorphism Problem (Easy)

$G = \mathrm{GL}_n$ acts on $\mathrm{Mat}_{n,n}^m$ by simultaneous conjugation
$A = (A_1, \ldots, A_m), A' = (A'_1, \ldots, A'_m) \in \mathrm{Mat}_{n,n}^m$

is there a $P \in \mathrm{GL}_n$ with $(PA_1P^{-1}, \ldots, PA_mP^{-1}) = (A'_1, \ldots, A'_m)$?

Module Isomorphism Problem (Easy)

$R = k\langle x_1, \dots, x_m \rangle$ free associative algebra
$(A_1, \dots, A_m) \in \mathrm{Mat}_{n,n}^m$ corresponds to module $M = k^n$,
where $x_i \cdot v = A_i v$ for $v \in M$

Module Isomorphism Problem (Easy)

$R = k\langle x_1, \ldots, x_m \rangle$ free associative algebra
$(A_1, \ldots, A_m) \in \mathrm{Mat}_{n,n}^m$ corresponds to module $M = k^n$,
where $x_i \cdot v = A_i v$ for $v \in M$

$(A'_1, \ldots, A'_m) \in \mathrm{Mat}_{n,n}^m$ corresponds to module $M' = k^n$
$\mathrm{Hom}_R(M, M') = \{P \in \mathrm{Mat}_{n,n} \mid \forall i \; PA_i = A'_i P\}$

Module Isomorphism Problem (Easy)

$R = k\langle x_1, \ldots, x_m\rangle$ free associative algebra
$(A_1, \ldots, A_m) \in \mathrm{Mat}_{n,n}^m$ corresponds to module $M = k^n$,
where $x_i \cdot v = A_i v$ for $v \in M$

$(A'_1, \ldots, A'_m) \in \mathrm{Mat}_{n,n}^m$ corresponds to module $M' = k^n$
$\mathrm{Hom}_R(M, M') = \{P \in \mathrm{Mat}_{n,n} \mid \forall i \; PA_i = A'_i P\}$

Probabilistic Module Isomorphism Algorithm

choose $P \in \mathrm{Hom}_R(M, M') \subseteq \mathrm{Mat}_{n,n}$ at random
if P invertible, then $M \cong M'$
if P not invertible, then $M \ncong M'$ with high probability

polynomial time de-randomized algorithms for module isom.:
Chistov-Ivanyos-Karpinsky 1997, Brooksbank-Luks 2008
(for arbitrary finitely generated associative k-algebras)

Graph Isomorphism by Solving Polynomial Equations

Γ, Γ' graphs on n vertices with adjacency matrices
$A = (a_{i,j}), A' = (a'_{i,j})$
does there exists a permutation $n \times n$ matrix $X = (x_{i,j})$ with
$XAX^{-1} = A'$?

Graph Isomorphism by Solving Polynomial Equations

Γ, Γ' graphs on n vertices with adjacency matrices $A = (a_{i,j}), A' = (a'_{i,j})$
does there exists a permutation $n \times n$ matrix $X = (x_{i,j})$ with $XAX^{-1} = A'$?

We need to solve a system of polynomial equations:

Graph Isomorphism by Solving Polynomial Equations

Γ, Γ' graphs on n vertices with adjacency matrices
$A = (a_{i,j}), A' = (a'_{i,j})$
does there exists a permutation $n \times n$ matrix $X = (x_{i,j})$ with
$XAX^{-1} = A'$?

We need to solve a system of polynomial equations:

X is a permutation matrix, means:
(1) $x_{i,j}x_{i,\ell} = 0 = x_{j,i}x_{\ell,i}$ for all i and all $j \neq \ell$
(2) $\sum_{j=1}^{n} x_{i,j} - 1 = \sum_{j=1}^{n} x_{j,i} - 1 = 0$ for all i

Graph Isomorphism by Solving Polynomial Equations

Γ, Γ' graphs on n vertices with adjacency matrices
$A = (a_{i,j}), A' = (a'_{i,j})$
does there exists a permutation $n \times n$ matrix $X = (x_{i,j})$ with
$XAX^{-1} = A'$?

We need to solve a system of polynomial equations:

X is a permutation matrix, means:
(1) $x_{i,j}x_{i,\ell} = 0 = x_{j,i}x_{\ell,i}$ for all i and all $j \neq \ell$
(2) $\sum_{j=1}^{n} x_{i,j} - 1 = \sum_{j=1}^{n} x_{j,i} - 1 = 0$ for all i

$XA = A'X$ gives us the linear equations:
(3) $\sum_{j=1} x_{i,j}a_{j,\ell} - \sum_{j=1} a'_{i,j}x_{j,\ell} = 0$ for all i, ℓ

system of linear and quadratic equations in n^2 variables

Gröbner Basis?

$R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ polynomial ring in n^2 variables
define $\mathrm{Eq}(\Gamma, \Gamma') \subset R$ as the set of poly's from our system of equations (1)-(3)
let $I = (\mathrm{Eq}(\Gamma, \Gamma')) \subseteq R$ be the ideal generated by $\mathrm{Eq}(\Gamma, \Gamma')$

Hilbert's Nullstellensatz

$$1 \in I \Leftrightarrow \Gamma \ncong \Gamma'$$

Gröbner Basis?

$R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ polynomial ring in n^2 variables
define $\mathrm{Eq}(\Gamma, \Gamma') \subset R$ as the set of poly's from our system of equations (1)-(3)
let $I = (\mathrm{Eq}(\Gamma, \Gamma')) \subseteq R$ be the ideal generated by $\mathrm{Eq}(\Gamma, \Gamma')$

Hilbert's Nullstellensatz

$$1 \in I \Leftrightarrow \Gamma \ncong \Gamma'$$

Algorithm 1, Gröbner basis (GB)

compute Gröbner basis $\mathcal{G}$ of I using Buchberger's algorithm
then $1 \in \mathcal{G} \Leftrightarrow 1 \in I \Leftrightarrow \Gamma \ncong \Gamma'$

Gröbner Basis?

$R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ polynomial ring in n^2 variables
define $\mathrm{Eq}(\Gamma, \Gamma') \subset R$ as the set of poly's from our system of equations (1)-(3)
let $I = (\mathrm{Eq}(\Gamma, \Gamma')) \subseteq R$ be the ideal generated by $\mathrm{Eq}(\Gamma, \Gamma')$

Hilbert's Nullstellensatz

$$1 \in I \Leftrightarrow \Gamma \ncong \Gamma'$$

Algorithm 1, Gröbner basis (GB)

compute Gröbner basis $\mathcal{G}$ of I using Buchberger's algorithm
then $1 \in \mathcal{G} \Leftrightarrow 1 \in I \Leftrightarrow \Gamma \ncong \Gamma'$

Computing a Gröbner basis is known to be **very** slow
there is no reason to believe Algorithm 1 could be polynomial time
This is a stupid approach!

Truncated Ideals

. . . or is it?

Truncated Ideals

. . . or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

Truncated Ideals

. . . or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

$R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$ space of polynomials of degree $\leq d$
$\dim R_d$ is polynomial in n (for fixed d)

Truncated Ideals

. . . or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

$R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$ space of polynomials of degree $\leq d$
dim R_d is polynomial in n (for fixed d)

we construct subspaces $I^{[0]} \subseteq I^{[1]} \subseteq \cdots$ of R_d as follows:

- $I^{[0]} \subseteq R_d$ is the k-span of $\mathrm{Eq}(\Gamma, \Gamma')$
  ($\mathrm{Eq}(\Gamma, \Gamma')$ was the set of linear and quadratic equations)

Truncated Ideals

. . . or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

$R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$ space of polynomials of degree $\leq d$
dim R_d is polynomial in n (for fixed d)

we construct subspaces $I^{[0]} \subseteq I^{[1]} \subseteq \cdots$ of R_d as follows:

- $I^{[0]} \subseteq R_d$ is the k-span of $\mathrm{Eq}(\Gamma, \Gamma')$
  ($\mathrm{Eq}(\Gamma, \Gamma')$ was the set of linear and quadratic equations)
- $I^{[j+1]} = \sum_{e=0}^{d} (I^{[j]} \cap R_e) R_{d-e}$ for all j

Truncated Ideals

. . . or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

$R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$ space of polynomials of degree $\leq d$
dim R_d is polynomial in n (for fixed d)

we construct subspaces $I^{[0]} \subseteq I^{[1]} \subseteq \cdots$ of R_d as follows:

- $I^{[0]} \subseteq R_d$ is the k-span of $\mathrm{Eq}(\Gamma, \Gamma')$
  ($\mathrm{Eq}(\Gamma, \Gamma')$ was the set of linear and quadratic equations)
- $I^{[j+1]} = \sum_{e=0}^{d} (I^{[j]} \cap R_e) R_{d-e}$ for all j

Truncated Ideals

...or is it?

we restrict ourselves to computations in low degree
fix positive integer $d \geq 2$

$R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$ space of polynomials of degree $\leq d$
$\dim R_d$ is polynomial in n (for fixed d)

we construct subspaces $I^{[0]} \subseteq I^{[1]} \subseteq \cdots$ of R_d as follows:

- $I^{[0]} \subseteq R_d$ is the k-span of $\mathrm{Eq}(\Gamma, \Gamma')$
  ($\mathrm{Eq}(\Gamma, \Gamma')$ was the set of linear and quadratic equations)
- $I^{[j+1]} = \sum_{e=0}^{d} (I^{[j]} \cap R_e) R_{d-e}$ for all j

for some $\ell \leq \dim R_d$, $I^{[\ell]} = I^{[\ell+1]} = I^{[\ell+2]} = \cdots$
Let $(\mathrm{Eq}(\Gamma, \Gamma'))_d = I^{[\ell]}$ be this limit
this is the d-truncated ideal generated by $\mathrm{Eq}(\Gamma, \Gamma')$

Comparison to the Weisfeiler-Leman Algorithm

a basis of $(\mathrm{Eq}(\Gamma, \Gamma'))_d$ (as a k-vector space) can be computed with a polynomial number of arithmetic operations in the field k

Algorithm 2, Truncated Ideals ($\mathbf{TI}_d$)

compute $(\mathrm{Eq}(\Gamma, \Gamma'))_d$ and test whether $1 \in (\mathrm{Eq}(\Gamma, \Gamma'))_d$
if $1 \in (\mathrm{Eq}(\Gamma, \Gamma'))_d$ then $\Gamma \not\cong \Gamma'$

Comparison to the Weisfeiler-Leman Algorithm

a basis of $(\mathrm{Eq}(\Gamma, \Gamma'))_d$ (as a k-vector space) can be computed with a polynomial number of arithmetic operations in the field k

Algorithm 2, Truncated Ideals ($\mathbf{TI}_d$)

compute $(\mathrm{Eq}(\Gamma, \Gamma'))_d$ and test whether $1 \in (\mathrm{Eq}(\Gamma, \Gamma'))_d$
if $1 \in (\mathrm{Eq}(\Gamma, \Gamma'))_d$ then $\Gamma \not\cong \Gamma'$

this algorithm is polynomial time if we work over a finite field $k = \mathbb{F}_q$ and $q = q(n) = 2^{O(\mathrm{poly}(n))}$

Theorem

if q is a prime $> n$, $k = \mathbb{F}_q$
if $\mathbf{WL}_d$ distinguishes Γ and Γ', then $\mathbf{TI}_{2d+2}$ distinguishes Γ and Γ'
*so **TI** is as powerful as **WL** (but perhaps not more powerful)*

but there is more structure ...

An Associative Algebra

recall $R = k[x_{1,1}, x_{1,2}, \dots, x_{n,n}]$ and $R_d = k[x_{1,1}, x_{1,2}, \dots, x_{n,n}]_{\leq d}$
matrix multiplication gives a ring homomorphism

$$\varphi : R = k[x_{1,1}, \dots, x_{n,n}] \to k[y_{1,1}, \dots, y_{n,n}, z_{1,1}, \dots, z_{n,n}] \cong R \otimes R$$

defined by $\varphi(x_{i,j}) = \sum_{\ell=1}^{n} y_{i,\ell} z_{\ell,j}$

An Associative Algebra

recall $R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ and $R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$
matrix multiplication gives a ring homomorphism

$$\varphi : R = k[x_{1,1}, \ldots, x_{n,n}] \to k[y_{1,1}, \ldots, y_{n,n}, z_{1,1}, \ldots, z_{n,n}] \cong R \otimes R$$

defined by $\varphi(x_{i,j}) = \sum_{\ell=1}^{n} y_{i,\ell} z_{\ell,j}$
this ring homomorphism restricts to a linear map $R_d \to R_d \otimes R_d$,

An Associative Algebra

recall $R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ and $R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$
matrix multiplication gives a ring homomorphism

$$\varphi : R = k[x_{1,1}, \ldots, x_{n,n}] \to k[y_{1,1}, \ldots, y_{n,n}, z_{1,1}, \ldots, z_{n,n}] \cong R \otimes R$$

defined by $\varphi(x_{i,j}) = \sum_{\ell=1}^{n} y_{i,\ell} z_{\ell,j}$
this ring homomorphism restricts to a linear map $R_d \to R_d \otimes R_d$,
which dualizes to a linear map $R_d^\star \otimes R_d^\star \to R_d^\star$,

An Associative Algebra

recall $R = k[x_{1,1}, x_{1,2}, \dots, x_{n,n}]$ and $R_d = k[x_{1,1}, x_{1,2}, \dots, x_{n,n}]_{\leq d}$
matrix multiplication gives a ring homomorphism

$$\varphi : R = k[x_{1,1}, \dots, x_{n,n}] \to k[y_{1,1}, \dots, y_{n,n}, z_{1,1}, \dots, z_{n,n}] \cong R \otimes R$$

defined by $\varphi(x_{i,j}) = \sum_{\ell=1}^{n} y_{i,\ell} z_{\ell,j}$
this ring homomorphism restricts to a linear map $R_d \to R_d \otimes R_d$,
which dualizes to a linear map $R_d^\star \otimes R_d^\star \to R_d^\star$,
which defines a bilinear multiplication $R_d^\star \times R_d^\star \to R_d^\star$,

An Associative Algebra

recall $R = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]$ and $R_d = k[x_{1,1}, x_{1,2}, \ldots, x_{n,n}]_{\leq d}$
matrix multiplication gives a ring homomorphism

$$\varphi : R = k[x_{1,1}, \ldots, x_{n,n}] \to k[y_{1,1}, \ldots, y_{n,n}, z_{1,1}, \ldots, z_{n,n}] \cong R \otimes R$$

defined by $\varphi(x_{i,j}) = \sum_{\ell=1}^{n} y_{i,\ell} z_{\ell,j}$
this ring homomorphism restricts to a linear map $R_d \to R_d \otimes R_d$,
which dualizes to a linear map $R_d^\star \otimes R_d^\star \to R_d^\star$,
which defines a bilinear multiplication $R_d^\star \times R_d^\star \to R_d^\star$,
which makes $R_d^\star$ into an associative algebra

The Category $\mathcal{C}_{n,d}$

Definition (Approximate Category $\mathcal{C}_{n,d}$)

objects of $\mathcal{C}_{n,d}$ are graphs on n vertices,

Definition (Approximate Category $\mathcal{C}_{n,d}$)

objects of $\mathcal{C}_{n,d}$ are graphs on n vertices,

$$\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') = (R_d/(\mathrm{Eq}(\Gamma, \Gamma'))_d)^\star \subseteq R_d^\star$$

The Category $\mathcal{C}_{n,d}$

Definition (Approximate Category $\mathcal{C}_{n,d}$)

objects of $\mathcal{C}_{n,d}$ are graphs on n vertices,

$$\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') = (R_d/(\mathrm{Eq}(\Gamma, \Gamma'))_d)^\star \subseteq R_d^\star$$

multiplication $R_d^\star \times R_d^\star \to R_d^\star$ restricts to a bilinear map

$$\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') \times \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma', \Gamma'') \to \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma'')$$

Definition (Approximate Category $\mathcal{C}_{n,d}$)

objects of $\mathcal{C}_{n,d}$ are graphs on n vertices,

$$\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma,\Gamma') = (R_d/(\mathrm{Eq}(\Gamma,\Gamma'))_d)^\star \subseteq R_d^\star$$

multiplication $R_d^\star \times R_d^\star \to R_d^\star$ restricts to a bilinear map

$$\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma,\Gamma') \times \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma',\Gamma'') \to \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma,\Gamma'')$$

if $1 \in (\mathrm{Eq}(\Gamma,\Gamma'))_d$ then $(\mathrm{Eq}(\Gamma,\Gamma'))_d = R_d$ and $\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma,\Gamma') = 0$

Properties of $\mathcal{C}_{n,d}$

suppose Γ, Γ' graphs on n vertices with adjacency matrices A, A'
if $\Gamma \cong \Gamma'$ then there is a permutation matrix P with $PA = A'P$

Properties of $\mathcal{C}_{n,d}$

suppose Γ, Γ' graphs on n vertices with adjacency matrices A, A'
if $\Gamma \cong \Gamma'$ then there is a permutation matrix P with $PA = A'P$
if $\mathrm{ev}_P : R_d \to k$ is evaluation at P, then $\mathrm{ev}_P \in \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') \subseteq R_d^\star$
and ev_P is an isomorphism in $\mathcal{C}_{n,d}$ (with inverse $\mathrm{ev}_{P^{-1}}$)

Properties of $\mathcal{C}_{n,d}$

suppose Γ, Γ' graphs on n vertices with adjacency matrices A, A'
if $\Gamma \cong \Gamma'$ then there is a permutation matrix P with $PA = A'P$
if $\mathrm{ev}_P : R_d \to k$ is evaluation at P, then $\mathrm{ev}_P \in \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') \subseteq R_d^\star$
and ev_P is an isomorphism in $\mathcal{C}_{n,d}$ (with inverse $\mathrm{ev}_{P^{-1}}$)

Theorem

let $T = \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *(an associative k-algebra)*
Γ, Γ' *are isomorphic in* $\mathcal{C}_{n,d} \Leftrightarrow \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma', \Gamma)$ *and* $\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *are isomorphic* T*-modules*

Properties of $\mathcal{C}_{n,d}$

suppose Γ, Γ' graphs on n vertices with adjacency matrices A, A'
if $\Gamma \cong \Gamma'$ then there is a permutation matrix P with $PA = A'P$
if $\mathrm{ev}_P : R_d \to k$ is evaluation at P, then $\mathrm{ev}_P \in \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') \subseteq R_d^\star$
and ev_P is an isomorphism in $\mathcal{C}_{n,d}$ (with inverse $\mathrm{ev}_{P^{-1}}$)

Theorem

let $T = \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *(an associative k-algebra)*
Γ, Γ' *are isomorphic in* $\mathcal{C}_{n,d} \Leftrightarrow \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma', \Gamma)$ *and* $\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *are isomorphic* T*-modules*

we can test whether Γ, Γ' are isomorphic in $\mathcal{C}_{n,d}$ in polynomial time

Properties of $\mathcal{C}_{n,d}$

suppose Γ, Γ' graphs on n vertices with adjacency matrices A, A'
if $\Gamma \cong \Gamma'$ then there is a permutation matrix P with $PA = A'P$
if $\mathrm{ev}_P : R_d \to k$ is evaluation at P, then $\mathrm{ev}_P \in \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma') \subseteq R_d^\star$
and ev_P is an isomorphism in $\mathcal{C}_{n,d}$ (with inverse $\mathrm{ev}_{P^{-1}}$)

Theorem

let $T = \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *(an associative* k*-algebra)*
Γ, Γ' *are isomorphic in* $\mathcal{C}_{n,d} \Leftrightarrow \mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma', \Gamma)$ *and* $\mathrm{Hom}_{\mathcal{C}_{n,d}}(\Gamma, \Gamma)$ *are isomorphic* T*-modules*

we can test whether Γ, Γ' are isomorphic in $\mathcal{C}_{n,d}$ in polynomial time

Algorithm 3 ($\mathbf{AC}_d$)

test whether Γ, Γ' are isomorphic in the category $\mathcal{C}_{n,d}$ for all fields $k = \mathbb{F}_q$ with q a prime $\leq 2n$
if not isomorphic for some k, then Γ and Γ' are non-isomorphic graphs

if $V=\{1,2,\ldots,n\}$ is the set of vertices, then $\mathbf{WL}_{d-1}$ captures reasoning on subsets of V^d
it is as powerful as d-variable logic with counting (see Cai-Fürer-Immerman)

if $W=kV\cong k^n$ is the vector space whose basis is the set of vertices, then $\mathbf{AC}_{2d}$ captures reasoning with subspaces of $W^{\otimes d}=W\otimes\cdots\otimes W$ with operations such as tensor products, sums, intersections, projections and dimension count.

Cai-Fürer-Immerman constructed families of pairs of nonisomorphic graphs that cannot be distinguished by $\mathbf{WL}_d$ for any fixed d
so $\mathbf{WL}_d$ does not give a polynomial time algorithm

for a pair of CFI graphs (Γ, Γ'), we can construct matrices B and B' from the adjacency matrices A and A' such that B and B' do not have the same rank if $k = \mathbb{F}_2$
$\mathbf{AC}_3$ can distinguish each pair of CFI-graphs (Γ, Γ') if we work over $k = \mathbb{F}_2$