Isomorphism problems in algebra

Nitin Saxena

Department of CSE

Indian Institute of Technology Kanpur

UPMC Paris, 2014

Contents

Motivation

- Let A be a commutative algebra, over a commutative unital ring R.
  - Assume that A over R has finitely many generators.
  - Eg. $A=R[x]/\langle x^2-a\rangle$, for $R=Z/nZ$.
- Algebra Isomorphism: Given two such R-algebras A_1, A_2 in the input, can we test them for isomorphism?
  - Natural question!
  - Is $\mathbb{Q}$-algebra isomorphism even computable?
  - Captures several major open problems in computation.
  - Eg. graph isomorphism, polynomial isomorphism, integer factoring, polynomial factoring.

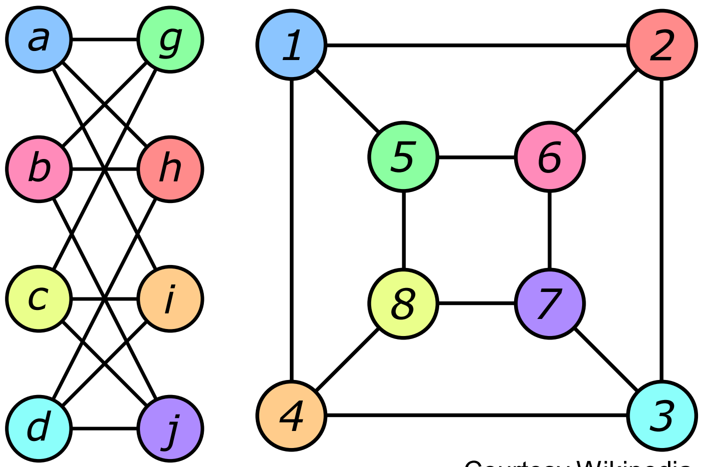
Motivation

- Alg.isomorphism, over *finite fields*, is not believed to be NP-hard.
  - It is in NP.
  - It is also in “randomized coNP”, i.e. coAM.
  - It's a problem of “intermediate” complexity.
- Similar is the status of graph isomorphism (GI).
  - GI is easy for random input graphs.
  - Alg.isomorphism doesn't seem so.
  - No subexponential algorithms known in *quantum computing*.
- Applications: Chemical database search, electronic circuits design, cryptosystems, hardness of polynomials (Mulmuley's GCT), invariant theory,....

Contents

Graphs, polynomials and algebras

- GI is a well studied problem, with a long history.
  - One way could be to come up with a canonical form of a graph.
  - There might be *less direct*, more computational ways to solve GI.



Courtesy Wikipedia

- There are reductions to algebraic isomorphism problems.

- For a graph $G=([n],E)$ we can consider the polynomial $p_G := \sum_{(i,j) \in E} x_i x_j$.

- [Thierauf 1998] Graphs G, G' are isomorphic iff p_G , $p_{G'}$ are isomorphic (up to variable *permutations*).

Graphs, polynomials and algebras

- This reduction can be made algebraically nicer!
  - By using it to define an algebra.
- For the graph $G=([n],E)$, the polynomial $p_G := \sum_{(i,j) \in E} x_i x_j$, define an algebra $A(G) := F[x_1,\ldots,x_n]/\langle p_G, x_i^2, x_i x_j x_k \mid i,j,k\rangle$.
  - Char(F) $\neq 2$.
- [Agrawal,S 2005] Graphs G, G' are isomorphic iff A(G), A(G') are isomorphic algebras.
  - *Proof:* ($\Leftarrow$) Show that any isomorphism φ is, essentially, a permutation on the variables.
- $A(G)$ is a *commutative*, *local*, F-algebra with nilpotency index *three*.

Contents

- Motivation
- Graphs & algebras
- Quadratic forms
- Cubic forms
- Polynomial isomorphism
- Conclusion

Quadratic forms

- Let $f_1, f_2 \in F[x_1, \ldots, x_n] = F[\mathbf{x}]$ be quadratic polynomials.
  - Called isomorphic, $f_1 \sim f_2$, if there is an *invertible* matrix A s.t. $f_1(A\mathbf{x}) = f_2$.
  - Eg. over $\mathbb{Q}$, $\{x_1^2, x_1x_2\}$ are *not* isomorphic, but $\{x_1^2 - x_2^2, x_1x_2\}$ *are*.
  - Char(F) $\neq 2$.
  - Suffices to consider the diagonal form $\sum_{i \in [n]} a_i x_i^2$.
- Quad.forms Isomorphism: Given quadratic forms f_1, f_2 in the input, can we test them for isomorphism?
- It is a well understood problem due to the classical works of Minkowski (1885), Hasse (1921), and Witt (1937).

Quadratic forms

- Over $\mathbb{C}$, a quadratic form $\sum_{i \in [n]} a_i x_i^2$ is isomorphic to $\sum_{i \in [n]} x_i^2$.
  - Isomorphism testing boils down to counting the variables!
- Over $\mathbb{Q}$ and F_q the problem is highly nontrivial.
  - Historically, the algorithm has two parts – *Root finding* and *Witt decomposition*.
- Root finding: If $\sum_{i \in [n]} a_i x_i^2 \sim \sum_{i \in [n]} b_i x_i^2$, then the isomorphism would *contain* a root of the equation $\sum_{i \in [n]} a_i Y_i^2 = b_1$.
  - How to find a root of a quadratic equation?

Quadratic forms – root finding

- Over *finite fields*, a *random* setting of all, but one, variables in $\sum_{i \in [n]} a_i Y_i^2 = b_1$ would yield a root!
  - Weil's character sum estimates from 1940s.
  - Root finding is in randomized poly-time.

- Over *rationals*, it boils down to solving $a_1 Y_1^2 + a_2 Y_2^2 = 1$.
  - Legendre gave a classical method, using Lagrange's descent, to solve this.
  - The starting point is to compute $\sqrt{a_1} \bmod a_2$.
  - Given an oracle for integer factorization, root finding is in randomized poly-time.

Quadratic forms – Witt decomposition

- Once we've a root $\boldsymbol{\alpha}$ of $\sum_{i \in [n]} a_i Y_i^2 = b_1$, Witt's decomposition, and *cancellation*, reduces the isomorphism question to $\sum_{i \in [n-1]} a'_i x_i^2 \sim \sum_{i \in [2...n]} b_i x_i^2$?
  - Associate the form $\sum_{i \in [n]} a_i x_i^2$ with a symmetric bilinear map $\Theta: F^n \times F^n \to F^n$.
  - Consider the smaller subspace $U := \{ u \in F^n \mid \Theta(\boldsymbol{\alpha}, u)=0 \}$.
  - The $(n-1)$-variate quadratic form to consider is $\Theta(U,U)$.

- These classical tools give us a randomized poly-time algorithm to find an isomorphism between quadratic forms –
  - Over finite fields.
  - Over rationals, *assuming integer factorization*.

- [Wallenborn,S 2013] Equivalence with integer factorization.

Contents

Cubic forms

- Let $f_1, f_2 \in F[x_1, \ldots, x_n] = F[\mathbf{x}]$ be cubic polynomials.
  - Called isomorphic, $f_1 \sim f_2$, if there is an *invertible* matrix A s.t. $f_1(A\mathbf{x}) = f_2$.
  - Eg. over $\mathbb{Q}$, $\{ x_1^3 + x_1^2 x_2, x_2^3 + x_1^2 x_2 \}$ are *not* isomorphic, but $\{ x_1^3 + x_1^2 x_2, x_1^2 x_2 \}$ *are*.
  - Char(F) $\neq 2, 3$.
- Cubic forms isomorphism is not understood, over any field!
  - Issue-1: Cannot be diagonalized. Eg. $x_1^2 x_2$.
- Root finding of quadratic eqns reduced to questions *modulo primes*.
  - Local-global principle for a quadratic equation, over rationals.
  - False for cubics (Selmer'57). Trivial in ≥ 14 variables (Heath-Brown 2007).

Cubic forms

- Over $\mathbb{C}$, cubic forms isomorphism gives an algebraic system $f_1(A\mathbf{x}) = f_2(\mathbf{x})$ in the unknowns A.
  - If we denote the corresponding ideal by I, then the question is $1 \notin I$? (Hilbert's Nullstellensatz)
  - A linear algebraic way to solve it in PSPACE.

- Over *finite fields*, cubic forms isomorphism is in $NP \cap coAM$.
  - It's a problem of “intermediate” complexity.

- Over *rationals*, is cubic forms isomorphism even computable?
  - Note that solving algebraic equations, over rationals, is *not known* to be computable.
  - [Matiyasevich'70] Solving algebraic equations, over *integers*, is *uncomputable*.

Cubic forms – lower bound

- [Agrawal,S 2006] Commutative F-algebra isomorphism *reduces to* cubic forms isomorphism.
- An F-algebra R is given by a *formal* additive basis $\{b_1,\ldots,b_n\}$.
  - The multiplicative structure is *compactly* specified as, for all $i, j \in [n]$, $b_i b_j = \sum_{k \in [n]} a_{i,j,k} b_k$.
  - R is an n dimensional algebra over F.

L(R) is commutative and *local*.

- First, we consider a related F-algebra $L(R) :=$ $F[\mathbf{z},\mathbf{b},u] / \langle p_3, up_2, u^2\rangle+\langle \mathbf{z},\mathbf{b},u\rangle^4$.
  - $p_3 := \sum_{i,j \in [n]} z_{i,j} b_i b_j$, $p_2 := \sum_{i,j \in [n]} z_{i,j} (\sum_{k \in [n]} a_{i,j,k} b_k)$.
- $R \cong S$ iff $L(R) \cong L(S)$.

Cubic forms – lower bound

- $R \cong S$ iff $L(R) \cong L(S)$.
  - *Proof idea*: ($\Leftarrow$) Show that the linear part of any isomorphism φ yields an isomorphism from R to S.

- Thus, we can as well assume R, S to be local commutative F-algebras.

- Now we define a cubic form $f_R(\mathbf{y},\mathbf{c},v) :=$

$$\sum_{i,j \in [n']} y_{i,j}\, c_i\, c_j - v \sum_{i,j \in [n']} y_{i,j} \left(\sum_{k \in [n']} a_{i,j,k}\, c_k\right) .$$

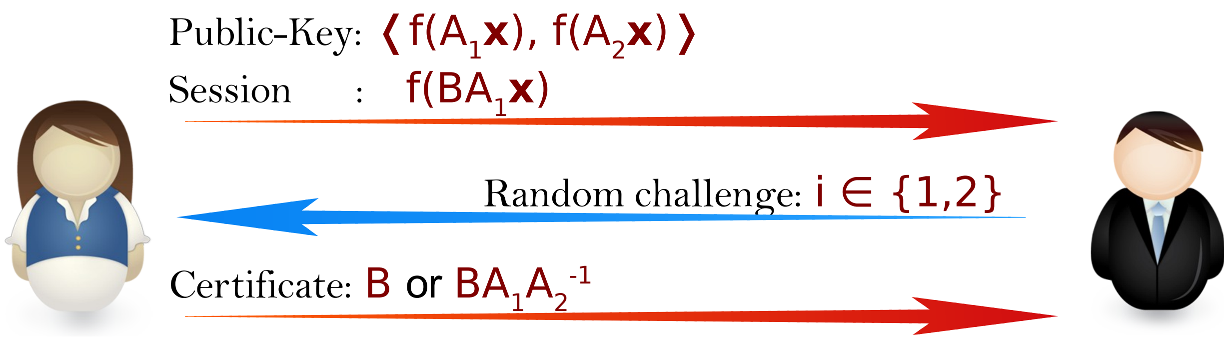
- A messy proof shows: $f_R \sim f_S$ iff $R \cong S$.

Cubic forms are *isomorphism hard* !

Contents

Polynomial isomorphism

- Let $f_1, f_2 \in F[x_1, ..., x_n] = F[\mathbf{x}]$ be degree d polynomials.
  - Specifying *equivalence classes* is a problem in invariant theory.
  - *Algorithmically*, can we improve the situation?
  - Clearly, at least as *hard* as cubic forms isomorphism.
- Patarin (1996) gave an authentication scheme –



- Cryptanalytic attacks are known by solving several cases of polynomial isomorphism:
  - [Kayal 2011] *Multilinear* f.
  - [Bouillaguet,Faugère,Fouque,Perret 2011] *Quadratic* and *cubic* f.

Polynomial isomorphism

- *Idea* in the *multilinear* case:
  Consider the space of 2nd-order partial derivatives of f_1 , f_2 .
- *Idea* in the *quadratic/ cubic* case:
  Analyze Gröbner basis method on a *random* input.
- It's not clear what to do in the worst-cases of multilinear or cubic polynomials.

Polynomial isomorphism

- In general, polynomial isomorphism has a status *similar* to that of cubic forms.
- *Morally*, polynomial isomorphism reduces to F-algebra isomorphism.
  - Thus, reduces to cubic forms equivalence.
- For a degree d form $f \in F[x_1, \ldots, x_n]$ define an F-algebra $L(f) := F[\mathbf{x}] / \langle f \rangle + \langle \mathbf{x} \rangle^{d+1}$.
- $L(f_1) \cong L(f_2) \quad \Leftrightarrow \quad f_1 \approx f_2$ (up to a constant multiple) .

Contents

- Motivation
- Graphs & algebras
- Quadratic forms
- Cubic forms
- Polynomial isomorphism
- Conclusion

Conclusion

- The isomorphism problems – of graphs, algebras, polynomials – are all related to those of cubic forms.
- Show that cubic forms isomorphism, over $\mathbb{Q}$, is computable.
- Is there a local-global principle for this problem?

Thank you !