The Complexity of Homomorphism Factorization

New Results Pertaining to General Algebraic Structures

Kevin M. Berg

University of Colorado Boulder

May 19, 2018

Outline

The Homomorphism Factorization Problem

We fix an algebraic language $\mathcal{L}$.

Problem (The Homomorphism Factorization Problem)

Given a homomorphism $f\colon X \to Z$ between $\mathcal{L}$-algebras X and Z and an intermediate $\mathcal{L}$-algebra Y, decide whether there are homomorphisms $g\colon X \to Y$ and $h\colon Y \to Z$ such that $f = hg$, as shown below.

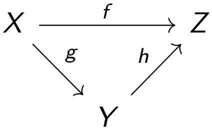


Figure: The commutative diagram for the homomorphism factorization problem.

Variants on the Homomorphism Factorization Problem

Problem (I. The Homomorphism Problem)

When $|Z| = 1$, the homomorphisms f and h from the HFP must be constant, reduces to the problem of deciding whether, given $\mathcal{L}$-algebras X and Y, there is a homomorphism $g\colon X \to Y$.

Variants on the Homomorphism Factorization Problem

Problem (I. The Homomorphism Problem)

When $|Z| = 1$, the homomorphisms f and h from the HFP must be constant, reduces to the problem of deciding whether, given $\mathcal{L}$-algebras X and Y, there is a homomorphism $g \colon X \to Y$.

Problem (II. The Find Right-Factor Problem)

Given $\mathcal{L}$-algebras X, Y, and Z, and homomorphisms $f \colon X \to Z$ and $h \colon Y \to Z$, decide whether there is a homomorphism $g \colon X \to Y$ such that $f = hg$.

Variants on the Homomorphism Factorization Problem

Problem (I. The Homomorphism Problem)

When $|Z| = 1$, the homomorphisms f and h from the HFP must be constant, reduces to the problem of deciding whether, given $\mathcal{L}$-algebras X and Y, there is a homomorphism $g\colon X \to Y$.

Problem (II. The Find Right-Factor Problem)

Given $\mathcal{L}$-algebras X, Y, and Z, and homomorphisms $f\colon X \to Z$ and $h\colon Y \to Z$, decide whether there is a homomorphism $g\colon X \to Y$ such that $f = hg$.

Problem (III. The Find Left-Factor Problem)

Given $\mathcal{L}$-algebras X, Y, and Z, and homomorphisms $f\colon X \to Z$ and $g\colon X \to Y$, decide whether there is a homomorphism $h\colon Y \to Z$ such that $f = hg$.

Variants on the Homomorphism Factorization Problem

Problem (IV. The Retraction Problem)

When $Z = X$, and f is the identity function, reduces to the problem of deciding if, given X and Y, the algebra X is a retract of Y.

Variants on the Homomorphism Factorization Problem

Problem (IV. The Retraction Problem)

When $Z = X$, and f is the identity function, reduces to the problem of deciding if, given X and Y, the algebra X is a retract of Y.

Problem (V. The Isomorphism Problem)

Restrict the retraction problem to the special case where $|X| = |Y|$.

Finite Semigroups

Remark (Semigroup Relational Structures)

If S is a semigroup, then S can also be thought of as a relational structure with a single ternary relation $\{(x, y, z) \in S^3 \mid z = xy\}$.

Finite Semigroups

Remark (Semigroup Relational Structures)

If S is a semigroup, then S can also be thought of as a relational structure with a single ternary relation $\{(x, y, z) \in S^3 \mid z = xy\}$.

Proposition (Homomorphisms on Semigroups)

A function $f : X \to Z$ between semigroups is an algebra homomorphism when X and Z are considered as algebras if and only if it is a relational homomorphism when X and Z are considered as relational structures. Therefore, the problem of deciding if a semigroup algebra homomorphism can be factored is the same as the problem of deciding if a semigroup relational homomorphism can be factored.

Some Remarks About Semigroups

The problem of deciding if a semigroup homomorphism can be factored is not the same as the problem of deciding if a homomorphism of relational structures, with one ternary relation, can be factored.

The latter problem involves relational structures that are not codings of semigroups.

Some Remarks About Semigroups

The problem of deciding if a semigroup homomorphism can be factored is not the same as the problem of deciding if a homomorphism of relational structures, with one ternary relation, can be factored.

The latter problem involves relational structures that are not codings of semigroups.

Proposition

The homomorphism problem for ternary relational structures is NP-complete.

Some Remarks About Semigroups

The problem of deciding if a semigroup homomorphism can be factored is not the same as the problem of deciding if a homomorphism of relational structures, with one ternary relation, can be factored.

The latter problem involves relational structures that are not codings of semigroups.

Proposition

The homomorphism problem for ternary relational structures is NP-complete.

Proposition (Homomorphism Problem for Semigroups)

Given finite semigroups X and Y, there is always a semigroup homomorphism $g\colon X \to Y$, given by g a constant homomorphism mapping X to an idempotent of Y.

Undirected Graphs

Definition (Undirected Graph)

An **undirected graph**, $G = (V_G, E_G)$, is a relational structure consisting of a universe, V_G, of vertices, together with a single binary relation, E_G, the set of edges of G.

Undirected Graphs

Definition (Undirected Graph)

An **undirected graph**, $G = (V_G, E_G)$, is a relational structure consisting of a universe, V_G, of vertices, together with a single binary relation, E_G, the set of edges of G.

Theorem (Graph Homomorphism)

Given two graphs, G and H, the question of whether there exists a relational homomorphism $\phi\colon G \to H$ is NP-Complete.

Graph Encoding into Non-Associative Magmas

Let $G = (V_G, E_G)$ be an undirected graph.

Graph Encoding into Non-Associative Magmas

Let $G = (V_G, E_G)$ be an undirected graph.

Definition (G^*)

We define a non-associative magma G^*. For every v in V_G, there are two elements, v_1 and v_2 in G^*; there are four distinguished elements, a, b, c, and d; and there is a 0. We then assign to G^* a single, non-associative binary operation, $\cdot$.

Multiplication Table for $\cdot$

For any distinct u, v in V_G, we have

$\cdot$	0	a	b	c	d	u_1	v_1	u_2	v_2
0	0	0	0	0	0	0	0	0	0
a	0	b	a	a	a	u_1	v_1	u_2	v_2
b	0	a	c	a	a	u_1	v_1	u_2	v_2
c	0	a	a	d	a	u_1	v_1	u_2	v_2
d	0	a	a	a	a	u_1	v_1	u_2	v_2
u_1	0	u_1	u_1	u_1	u_1	$*$	$*$	c	d
v_1	0	v_1	v_1	v_1	v_1	$*$	$*$	d	c
u_2	0	u_2	u_2	u_2	u_2	c	d	$\dagger$	$\dagger$
v_2	0	v_2	v_2	v_2	v_2	d	c	$\dagger$	$\dagger$

where $*$ is either $u_1 v_1 = v_1 u_1 = a$ if (u, v) is in E_G, or else $u_1 v_1 = v_1 u_1 = d$, and $\dagger$ is similarly either $u_2 v_2 = v_2 u_2 = b$ if (u, v) is an edge in the complete loopless graph on V_G, or d otherwise.

Graph Encoding into Semigroups

Let $G = (V_G, E_G)$ be an undirected graph.

Graph Encoding into Semigroups

Let $G = (V_G, E_G)$ be an undirected graph.

Definition (X_G)

The universe of X_G consists of an element, v, for each v in V_G; an element, $\chi_{u,v}$, for each u, v in V_G such that (u, v) is not an element of E_G (note that we adopt the convention $\chi_{u,v} = \chi_{v,u}$); distinct elements b, b^2, and c; and a 0. We assign to X_G the single binary operation, $\cdot$.

Graph Encoding into Semigroups

Let $G = (V_G, E_G)$ be an undirected graph.

Definition (X_G)

The universe of X_G consists of an element, v, for each v in V_G; an element, $\chi_{u,v}$, for each u, v in V_G such that (u, v) is not an element of E_G (note that we adopt the convention $\chi_{u,v} = \chi_{v,u}$); distinct elements b, b^2, and c; and a 0. We assign to X_G the single binary operation, $\cdot$.

Remark

Intuitively, X_G is a description of the graph, G, together with a new distinguished vertex, b, which is connected to all vertices of G.

Multiplication Table for $\cdot$

For any distinct u, v in V_G, we have

$\cdot$	0	b	b^2	c	u	v	χ
0	0	0	0	0	0	0	0
b	0	b^2	0	0	c	c	0
b^2	0	0	0	0	0	0	0
c	0	0	0	0	0	0	0
u	0	c	0	0	$*$	$*$	0
v	0	c	0	0	$*$	$*$	0
χ	0	0	0	0	0	0	0

where for any u and v in V_G, $*$ is either $uv = vu = c$ if (u, v) is in E_G, or else $uv = vu = \chi_{u,v}$; and χ is a placeholder for any $\chi_{u,v}$ in the semigroup.

Finite Non-Associative Algebras

Finite Non-Associative Algebras

Theorem (B., '18)

Let G and H be undirected graphs with at least two vertices. There exists a homomorphism $\phi\colon G \to H$ if and only if there exists a homomorphism $\psi\colon G^* \to H^*$.

Finite Non-Associative Algebras

Theorem (B., '18)

Let G and H be undirected graphs with at least two vertices. There exists a homomorphism $\phi\colon G \to H$ if and only if there exists a homomorphism $\psi\colon G^* \to H^*$.

Corollary

The homomorphism problem for finite non-associative algebras is NP-complete.

Finite Semigroups

Suppose we take as our input two undirected graphs, $G = (V_G, E_G)$ and $H = (V_H, E_H)$. We encode G and H into semigroups, X_G and Y_H, and define a special semigroup, Z, with a single binary operation, $\cdot$, given by

Finite Semigroups

Suppose we take as our input two undirected graphs, $G = (V_G, E_G)$ and $H = (V_H, E_H)$. We encode G and H into semigroups, X_G and Y_H, and define a special semigroup, Z, with a single binary operation, $\cdot$, given by

Definition (Z Multiplication Table)

$\cdot$	0	a	b	b^2	c
0	0	0	0	0	0
a	0	c	c	0	0
b	0	c	b^2	0	0
b^2	0	0	0	0	0
c	0	0	0	0	0

Finite Semigroups

Suppose we take as our input two undirected graphs, $G = (V_G, E_G)$ and $H = (V_H, E_H)$. We encode G and H into semigroups, X_G and Y_H, and define a special semigroup, Z, with a single binary operation, $\cdot$, given by

Definition (Z Multiplication Table)

$\cdot$	0	a	b	b^2	c
0	0	0	0	0	0
a	0	c	c	0	0
b	0	c	b^2	0	0
b^2	0	0	0	0	0
c	0	0	0	0	0

Remark

Z is equivalent to the encoding of the graph consisting of a single loop on a vertex a, but can also be thought of as an encoding of the two element graph that encodes independent sets as homomorphisms.

Finite Semigroups, Continued

We construct surjective homomorphisms $f\colon X_G \to Z$ and $h\colon Y_H \to Z$ by taking $f(0) = h(0) = 0$, $f(b) = h(b) = b$, $f(b^2) = h(b^2) = b^2$, and for any u in V_G or v in V_H, $f(u) = h(v) = a$, with all other elements going to c.

Finite Semigroups, Continued

We construct surjective homomorphisms $f\colon X_G \to Z$ and $h\colon Y_H \to Z$ by taking $f(0) = h(0) = 0$, $f(b) = h(b) = b$, $f(b^2) = h(b^2) = b^2$, and for any u in V_G or v in V_H, $f(u) = h(v) = a$, with all other elements going to c.

Theorem (B., '18)

There exists a homomorphism $g\colon X_G \to Y_H$ with $f = hg$ if and only if there exists a homomorphism $\phi\colon G \to H$.

Finite Semigroups, Continued

We construct surjective homomorphisms $f\colon X_G \to Z$ and $h\colon Y_H \to Z$ by taking $f(0) = h(0) = 0$, $f(b) = h(b) = b$, $f(b^2) = h(b^2) = b^2$, and for any u in V_G or v in V_H, $f(u) = h(v) = a$, with all other elements going to c.

Theorem (B., '18)

There exists a homomorphism $g\colon X_G \to Y_H$ with $f = hg$ if and only if there exists a homomorphism $\phi\colon G \to H$.

Corollary

The Find Right-Factor Problem for finite semigroups is NP-complete.

Operations of Higher and Lower Aritys

Let $G = (V_G, E_G)$ be an arbitrary, undirected graph. It is possible for the preceding homomorphism result to hold for alternate definitions of X_G using different operations.

Operations of Higher and Lower Aritys

Let $G = (V_G, E_G)$ be an arbitrary, undirected graph. It is possible for the preceding homomorphism result to hold for alternate definitions of X_G using different operations.

Theorem (B., '18)

Let X_G instead encode G with a single ternary operation.

Operations of Higher and Lower Aritys

Let $G = (V_G, E_G)$ be an arbitrary, undirected graph. It is possible for the preceding homomorphism result to hold for alternate definitions of X_G using different operations.

Theorem (B., '18)

Let X_G instead encode G with a single ternary operation.

Corollary

Let X_G instead encode G with a single n-ary operation for any $n \geq 3$.

Operations of Higher and Lower Aritys

Let $G = (V_G, E_G)$ be an arbitrary, undirected graph. It is possible for the preceding homomorphism result to hold for alternate definitions of X_G using different operations.

Theorem (B., '18)

Let X_G instead encode G with a single ternary operation.

Corollary

Let X_G instead encode G with a single n-ary operation for any $n \geq 3$.

Theorem (B., '18)

Let X_G instead encode G with an associative binary operation, $\cdot$, and a single unary operation, $\pi(\cdot)$.

Operations of Higher and Lower Aritys

We might naturally ask about the case of unary operations. However, because associativity does not apply for such algebras, and because we do not have sufficient arity for the previous non-associative example to hold, the problem is currently open in general. However, there is at least one case for which we know the Homomorphism Factorization Problem is in P.

Operations of Higher and Lower Aritys

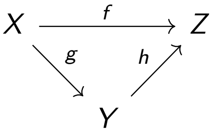
We might naturally ask about the case of unary operations. However, because associativity does not apply for such algebras, and because we do not have sufficient arity for the previous non-associative example to hold, the problem is currently open in general. However, there is at least one case for which we know the Homomorphism Factorization Problem is in P.

Problem (Open)

Suppose our algebras have only unary operations. Which variants (if any) of the Homomorphism Factorization Problem are NP-Complete for such algebras?

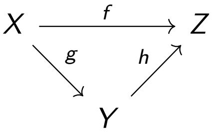
Bounded f-Cores

Recall our commutative diagram:



We consider a retraction $r\colon X \to X$ with the following property:

Recall our commutative diagram:



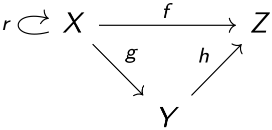
We consider a retraction $r\colon X \to X$ with the following property:

Definition

A retraction, r, **respects** f if $fr = f$.

Bounded f-Cores

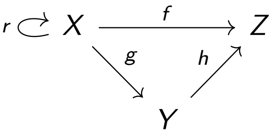
We now have the following diagram:



Let $X' = r(X)$. Since r respects f, we have:

Bounded f-Cores

We now have the following diagram:



Let $X' = r(X)$. Since r respects f, we have:

Proposition

f factors through Y if and only if $f|_{X'}$ factors through Y.

Bounded f-Cores

Clearly, this reduction can prove combinatorically useful. This motivates the following definitions:

Bounded f-Cores

Clearly, this reduction can prove combinatorically useful. This motivates the following definitions:

Definition (f-Core)

A is an f-**core** of X if A is minimal with respect to the existence of an onto, f-respecting retraction, $r\colon X \to A$, in a new language defined by taking the language of X together with all partitions of pairwise disjoint unary operations in the language. If X is its own f-core, we refer to X as an f-core.

Bounded f-Cores

Clearly, this reduction can prove combinatorically useful. This motivates the following definitions:

Definition (f-Core)

A is an f-**core** of X if A is minimal with respect to the existence of an onto, f-respecting retraction, $r\colon X \to A$, in a new language defined by taking the language of X together with all partitions of pairwise disjoint unary operations in the language. If X is its own f-core, we refer to X as an f-core.

Definition (Bounded f-Core)

We say a variety $\mathcal{V}$ has **bounded f-cores** if, for any finite algebra X in $\mathcal{V}$ and given a surjective map $f\colon X \to Z$ for which X is an f-core, the size of X is bounded by some function on the size of Z.

Bounded f-Cores

Let f be a function appropriately defined for a given variety.

Proposition (G-Sets)

Let G be a finite group. Then the variety of G-sets has bounded f-cores.

Bounded f-Cores

Let f be a function appropriately defined for a given variety.

Proposition (G-Sets)

Let G be a finite group. Then the variety of G-sets has bounded f-cores.

Proposition (Boolean Algebras)

Boolean algebras have bounded f-cores.

Bounded f-Cores

Let f be a function appropriately defined for a given variety.

Proposition (G-Sets)

Let G be a finite group. Then the variety of G-sets has bounded f-cores.

Proposition (Boolean Algebras)

Boolean algebras have bounded f-cores.

Proposition (Finite Vector Spaces)

Let F be a field. Then the variety of vector spaces over F has bounded f-cores.

Bounded f-Cores

Let f be a function appropriately defined for a given variety.

Proposition (G-Sets)

Let G be a finite group. Then the variety of G-sets has bounded f-cores.

Proposition (Boolean Algebras)

Boolean algebras have bounded f-cores.

Proposition (Finite Vector Spaces)

Let F be a field. Then the variety of vector spaces over F has bounded f-cores.

Proposition (Abelian Groups)

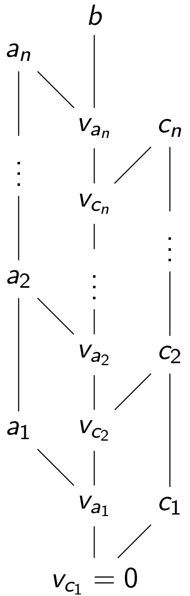
The variety of abelian groups has bounded f-cores.

Algebras Without Bounded f-Cores

Theorem (B., '18)

Consider the semilattice $S = (\{a, b, c, 0\}, \wedge)$ *given by* $a \wedge b = b \wedge c = a \wedge c = 0$*. Then for any natural number* n*, there exists a semilattice,* X*, of size at least* n *that is an* f*-core for a surjective* $f : X \to S$*.*

Algebras Without Bounded f-Cores



Bounded f-Cores and the Find Right-Factor Problem

We consider a special case of the Find Right-Factor Problem where the "target" algebra Z is fixed. In this case, if the size of X is bounded, we in turn bound the number of possible functions $g\colon X \to Y$, and thus are able to bound the number of steps required to produce such a g.

In fact, it suffices to check the weaker case where X has bounded f-cores with respect to Z. This motivates three questions we ask about bounded f-cores for this variation.

Bounded f-Cores and the Find Right-Factor Problem

We consider a special case of the Find Right-Factor Problem where the "target" algebra Z is fixed. In this case, if the size of X is bounded, we in turn bound the number of possible functions $g: X \to Y$, and thus are able to bound the number of steps required to produce such a g.

In fact, it suffices to check the weaker case where X has bounded f-cores with respect to Z. This motivates three questions we ask about bounded f-cores for this variation.

1. Are f-cores in a given variety bounded for finite algebras?

Bounded f-Cores and the Find Right-Factor Problem

We consider a special case of the Find Right-Factor Problem where the "target" algebra Z is fixed. In this case, if the size of X is bounded, we in turn bound the number of possible functions $g: X \to Y$, and thus are able to bound the number of steps required to produce such a g.

In fact, it suffices to check the weaker case where X has bounded f-cores with respect to Z. This motivates three questions we ask about bounded f-cores for this variation.

I. Are f-cores in a given variety bounded for finite algebras?
II. Can f-cores in a given variety be found for finite algebras in polynomial time?

Bounded f-Cores and the Find Right-Factor Problem

We consider a special case of the Find Right-Factor Problem where the "target" algebra Z is fixed. In this case, if the size of X is bounded, we in turn bound the number of possible functions $g \colon X \to Y$, and thus are able to bound the number of steps required to produce such a g.

In fact, it suffices to check the weaker case where X has bounded f-cores with respect to Z. This motivates three questions we ask about bounded f-cores for this variation.

I. Are f-cores in a given variety bounded for finite algebras?
II. Can f-cores in a given variety be found for finite algebras in polynomial time?
III. Can a retraction map from an arbitrary finite algebra to its f-core be found in polynomial time?

Bounded f-Cores and Polynomial Time Cases

Corollary

If conditions I through III are satisfied, then the Find Right-Factor problem can be solved in polynomial time for the given variety.

Bounded f-Cores and Polynomial Time Cases

Theorem (B., '18)

There exists a homomorphism $g\colon X \to Y$ if and only if there exists a homomorphism $g'\colon X' \to Y'$ where X' and Y' are the f-cores of X and Y, respectively.

Corollary

If conditions I through III are satisfied, then the Find Right-Factor problem can be solved in polynomial time for the given variety.

Complications

Several complications arose during the process of finding when conditions I through III hold. These complications entail interesting open questions about the nature of finite structures, as well as the computational complexity of Homomorphism Factorization Problems.

Complications

Several complications arose during the process of finding when conditions I through III hold. These complications entail interesting open questions about the nature of finite structures, as well as the computational complexity of Homomorphism Factorization Problems.

Theorem

Any algorithm that can find the f-core of an arbitrary relational structure, X, is capable of finding the three-coloring of an arbitrary graph, $G = (V_G, E_G)$.

Complications

Several complications arose during the process of finding when conditions I through III hold. These complications entail interesting open questions about the nature of finite structures, as well as the computational complexity of Homomorphism Factorization Problems.

Theorem

Any algorithm that can find the f-core of an arbitrary relational structure, X, is capable of finding the three-coloring of an arbitrary graph, $G = (V_G, E_G)$.

Proposition

There is at least one variety known to have unbounded f-cores.

Some Open Questions

Problem (Open)

Can the retraction map of X onto its f-core be determined in polynomial time?

Some Open Questions

Problem (Open)

Can the retraction map of X onto its f-core be determined in polynomial time?

Remark

Some known examples where this is the case already exist, and were presented earlier. Do these share some property that could be leveraged for a general result?

Some Open Questions

Problem (Open)

Can the retraction map of X onto its f-core be determined in polynomial time?

Remark

Some known examples where this is the case already exist, and were presented earlier. Do these share some property that could be leveraged for a general result?

Problem (Open)

What conditions must a variety satisfy to always have bounded f-cores? What conditions might be required of Z?

Thank You

Thank you for your time.