Results and speculations in the neighborhood of the flexible atom conjecture

Jeremy Alm

October 2016

Representable relation algebras

A *relation algebra* is an abstract algebra $\langle A, +, \cdot, ^{-}, ;, ^{\cup}, 1' \rangle$ satisfying several equational axioms.

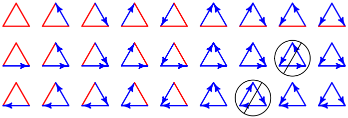
Representable relation algebras

A *relation algebra* is an abstract algebra $\langle A, +, \cdot, ^{-}, ;, ^{\cup}, 1' \rangle$ satisfying several equational axioms.

An algebra $\underline{A}$ is *representable* if there is an embedding $\underline{A} \to \langle P(E), \cup, \cap, ^{c}, |, ^{-1}, Id \rangle$, where E is some non-empty equivalence relation. The class RRA of representable algebras is a non-finitely based variety.

Diversity cycles

For integral algebras, the composition operation ; is determined by the diversity cycles:



This is the cycle structure for 33_{37}. The cycle $bb\breve{b}$ is forbidden. The red atom is flexible.

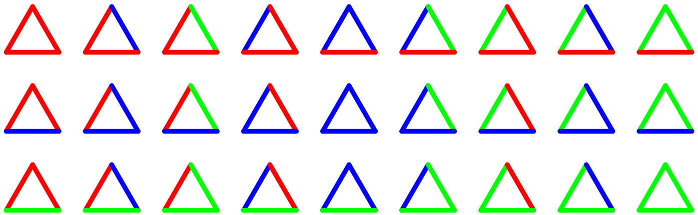
Flexible atoms

A diversity atom is called *flexible* if it does not participate in any forbidden cycle.

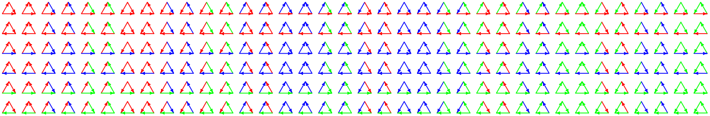
Flexible atoms

A diversity atom is called *flexible* if it does not participate in any forbidden cycle.

They can be symmetric...



. . . or directed (asymmetric):



Flexible atom conjecture

Theorem (Comer 1984)

Every finite integral RA with a flexible atom has a representation on a countable set.

Flexible atom conjecture

Theorem (Comer 1984)

Every finite integral RA with a flexible atom has a representation on a countable set.

Flexible atom conjecture

Every finite integral RA with a flexible atom has a representation on a FINITE set.

Results prior to 2016

- Jipsen, Maddux, Tuza 1995: the m-color all-flexible algebra is representable on a set of size $O(m^2)$

Results prior to 2016

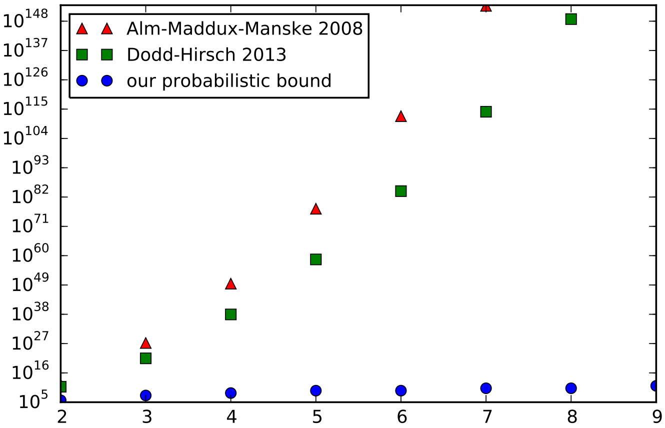
- Jipsen, Maddux, Tuza 1995: the m-color all-flexible algebra is representable on a set of size $O(m^2)$
- A., Maddux, Manske 2008: if all mandatory diversity cycles involve a single flexible atom, the algebra is representable on a (enormous) finite set

Results prior to 2016

- Jipsen, Maddux, Tuza 1995: the m-color all-flexible algebra is representable on a set of size $O(m^2)$
- A., Maddux, Manske 2008: if all mandatory diversity cycles involve a single flexible atom, the algebra is representable on a (enormous) finite set
- Dodd and Hirsch 2013: Lovász local lemma implies the sets can be less enormous

Results prior to 2016

- Jipsen, Maddux, Tuza 1995: the m-color all-flexible algebra is representable on a set of size $O(m^2)$
- A., Maddux, Manske 2008: if all mandatory diversity cycles involve a single flexible atom, the algebra is representable on a (enormous) finite set
- Dodd and Hirsch 2013: Lovász local lemma implies the sets can be less enormous
- A. and Sexton 2014: the sets can have size exponential in the number of colors


Alm-Maddux-Manske 2008
Dodd-Hirsch 2013
our probabilistic bound
10^{148}
10^{137}
10^{126}
10^{115}
10^{104}
10^{93}
10^{82}
10^{71}
10^{60}
10^{49}
10^{38}
10^{27}
10^{16}
10^{5}
2
3
4
5
6
7
8
9

New results

Theorem (A. 2016)

The m-color all-flexible algebra is representable over $\mathbb{Z}/p\mathbb{Z}$ *for every prime* $p \equiv 1 \pmod{2m}$ *greater than* m^4.

New results

Theorem (A. 2016)

The m-color all-flexible algebra is representable over $\mathbb{Z}/p\mathbb{Z}$ for every prime $p \equiv 1 \pmod{2m}$ greater than m^4.

The proof uses some Fourier-analytic methods along with a 1983 construction due to Comer.

Comer's method

Fix $m \in \mathbb{Z}^+$, and let $X_0 = H$ be a multiplicative subgroup of $\mathbb{F}_q^\times$, where $q \equiv 1 \pmod{m}$. Let $X_1, \ldots X_{m-1}$ be its cosets.

Comer's method

Fix $m \in \mathbb{Z}^+$, and let $X_0 = H$ be a multiplicative subgroup of $\mathbb{F}_q^\times$, where $q \equiv 1 \pmod{m}$. Let $X_1, \ldots X_{m-1}$ be its cosets.

Then define $A_i = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : x - y \in X_i\}$. Then the A_i's are the atoms of a proper RA over the base set $\mathbb{F}_q$. (Usually, q is prime, so $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

Comer's method

Fix $m \in \mathbb{Z}^+$, and let $X_0 = H$ be a multiplicative subgroup of $\mathbb{F}_q^\times$, where $q \equiv 1 \pmod{m}$. Let $X_1, \ldots X_{m-1}$ be its cosets.

Then define $A_i = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : x - y \in X_i\}$. Then the A_i's are the atoms of a proper RA over the base set $\mathbb{F}_q$. (Usually, q is prime, so $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

To figure out what the cycle structure is, use a computer!

A fast algorithm

The naive algorithm for computing the cycle structure runs in $O(p^2)$ (m fixed).

A fast algorithm

The naive algorithm for computing the cycle structure runs in $O(p^2)$ (m fixed).

However, the fact that

$$(X_0 + X_i) \cap X_j \neq \emptyset \implies (X_0 + X_i) \supseteq X_j$$

can be used to give an algorithm that runs in $O(p)$.

A fast algorithm

The naive algorithm for computing the cycle structure runs in $O(p^2)$ (m fixed).

However, the fact that

$$(X_0 + X_i) \cap X_j \neq \emptyset \Longrightarrow (X_0 + X_i) \supseteq X_j$$

can be used to give an algorithm that runs in $O(p)$.

Timing comparison:
for $m = 23$ and primes under 40000,

- naive took 22.7564027863 minutes

A fast algorithm

The naive algorithm for computing the cycle structure runs in $O(p^2)$ (m fixed).

However, the fact that

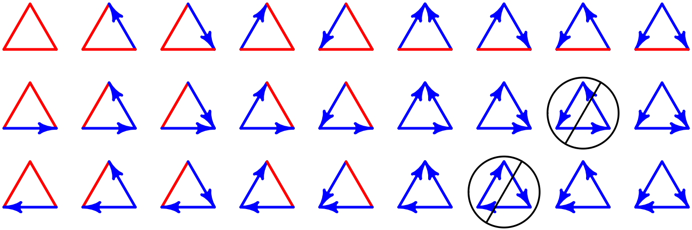
$$(X_0 + X_i) \cap X_j \neq \emptyset \Longrightarrow (X_0 + X_i) \supseteq X_j$$

can be used to give an algorithm that runs in $O(p)$.

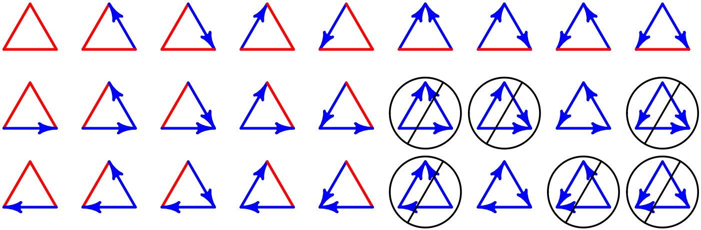
Timing comparison:
for $m = 23$ and primes under 40000,

- naive took 22.7564027863 minutes
- new took 6.86514431297 seconds

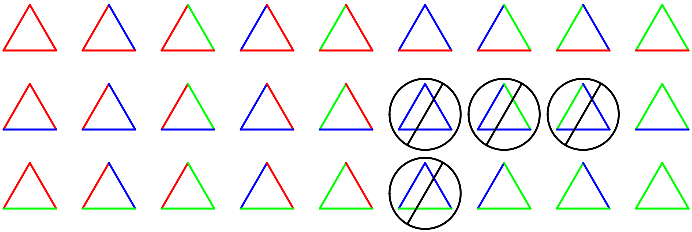
33_{37}



35_{37}



59_{65}



Some ad hoc constructions

Theorem (A. 2016)

- 33_{37} *is representable over* $\mathbb{Z}/p\mathbb{Z}$*, with* $p = 491, 661, 911, 1747, 2861\ldots$ *(over 700 moduli found so far)*

Some ad hoc constructions

Theorem (A. 2016)

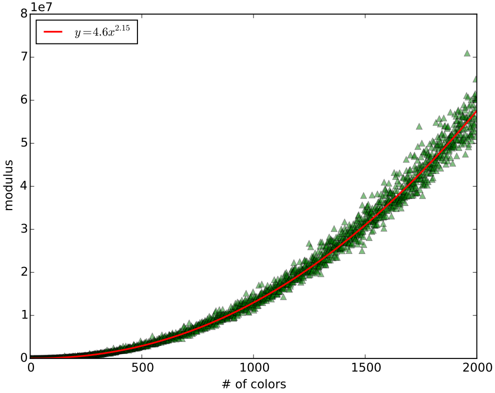
- 33_{37} *is representable over* $\mathbb{Z}/p\mathbb{Z}$, *with* $p = 491, 661, 911, 1747, 2861\ldots$ *(over 700 moduli found so far)*
- 35_{37} *is representable over* $\mathbb{Z}/p\mathbb{Z}$, *with* $p = 3221, 4231, 11527, 15319, 38011, 91873\ldots$

Some ad hoc constructions

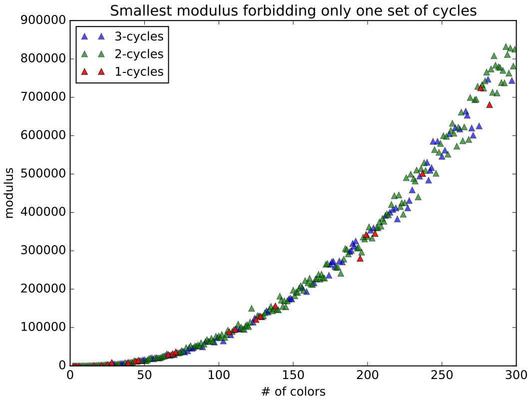
Theorem (A. 2016)

- 33_{37} *is representable over* $\mathbb{Z}/p\mathbb{Z}$, *with* $p = 491, 661, 911, 1747, 2861\ldots$ *(over 700 moduli found so far)*
- 35_{37} *is representable over* $\mathbb{Z}/p\mathbb{Z}$, *with* $p = 3221, 4231, 11527, 15319, 38011, 91873\ldots$
- 59_{65} *is representable over* $\mathbb{Z}/p\mathbb{Z}$, *with* $p = 113$

Forbidding $[i, i, i]$



Forbidding $[i, i+j, i+k]$



Speculations

- Primes behave "randomly"

Speculations

- Primes behave "randomly"
- Comer's algebras have "random" behavior

Questions

- Can Comer's algebras be shown to exhibit pseudorandom behavior?

Questions

- Can Comer's algebras be shown to exhibit pseudorandom behavior?
- Is there always a prime $p \equiv 1 \pmod{m}$ between m^2 and m^3? (This is where the most interesting stuff happens.)

Questions

- Can Comer's algebras be shown to exhibit pseudorandom behavior?
- Is there always a prime $p \equiv 1 \pmod{m}$ between m^2 and m^3? (This is where the most interesting stuff happens.)
- Which finite integral RAs can be embedded into an integral RA with n diversity atoms with an automorphism group that contains an n-cycle?