Automatized Construction of Implicative Theory of Algebraic Identities of Size up to 5

Artem Revenko

TU Dresden
HSE Moscow

ICFCA 2014
June 10

Formal Contexts & Implications

Definition (Formal Context)

M - a set of attributes.
G - a set of objects.
I - a relation between G and M.
$\mathbb{K} = (G, M, I)$ - a (formal) context.

	all sides equal	some sides equal	has right angle
◊	x	x	
□	x	x	x
▭		x	x
▱		x	

Formal Contexts & Implications

Definition (Formal Context)

M - a set of attributes.
G - a set of objects.
I - a relation between G and M.
$\mathbb{K} = (G, M, I)$ - a (formal) context.

	all sides equal	some sides equal	has right angle
◇	X	X	
□	X	X	X
▭		X	X
▱		X	

$\{\text{all sides equal}\} \rightarrow \text{some sides equal}$

(Unit) Implication $Y \rightarrow z$, $Y \subseteq M, z \in M$

$\forall g \in G :$ if gIY then gIz.

Formal Contexts & Implications

Definition (Formal Context)

M - a set of attributes.

G - a set of objects.

I - a relation between G and M.

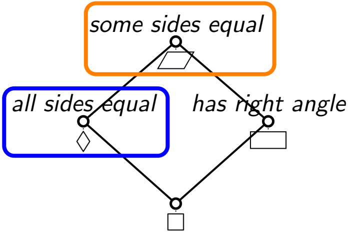
$\mathbb{K} = (G, M, I)$ - a (formal) context.

(Unit) Implication $Y \to z$, $Y \subseteq M, z \in M$

$\forall g \in G:$ if gIY then gIz.

	all sides equal	some sides equal	has right angle
◊	X	X	
□	X	X	X
▭		X	X
▱		X	

$\{$all sides equal$\} \to$ some sides equal



Implication Base

Implication base of context

Set of implications:

- from which any valid implication can be deduced,
- none of the proper subsets has this property.

Example

1. all sides equal $\to$ some sides equal;
2. has right angle $\to$ some sides equal.

Implication Base

Implication base of context

Set of implications:

- from which any valid implication can be deduced,
- none of the proper subsets has this property.

Example

1. all sides equal $\rightarrow$ some sides equal;
2. has right angle $\rightarrow$ some sides equal.

Counter-example

	all sides equal	some sides equal	has right angle
			x

Attribute Exploration of Quadrangles

	all sides equal	some sides equal	has right angle	all angles equal
	×	×		
	×	×	×	×
		×	×	×
		×		
				

1. all sides equal $\rightarrow$ some sides equal;
2. all angles equal $\rightarrow$ some sides equal, has right angle;
3. has right angle $\rightarrow$ some sides equal, all angles equal.

Attribute Exploration of Quadrangles

	all sides equal	some sides equal	has right angle	all angles equal
	x	x		
	x	x	x	x
		x	x	x
		x		
				
			x	

1. all sides equal $\rightarrow$ some sides equal;
2. all angles equal $\rightarrow$ some sides equal, has right angle;
3. has right angle $\rightarrow$ some sides equal, all angles equal.

Attribute Exploration of Quadrangles

	all sides equal	some sides equal	has right angle	all angles equal
	×	×		
	×	×	×	×
		×	×	×
		×		
				
			×	

1. all sides equal $\to$ some sides equal;
2. all angles equal $\to$ some sides equal, has right angle;
3. has right angle, some sides equal $\to$ all angles equal.

Attribute Exploration of Quadrangles

	all sides equal	some sides equal	has right angle	all angles equal
	x	x		
	x	x	x	x
		x	x	x
		x		
				
			x	
		x	x	

1. all sides equal $\rightarrow$ some sides equal;
2. all angles equal $\rightarrow$ some sides equal, has right angle;
3. has right angle, some sides equal $\rightarrow$ all angles equal.

Attribute Exploration of Quadrangles

	all sides equal	some sides equal	has right angle	all angles equal
	x	x		
	x	x	x	x
		x	x	x
		x		
				
			x	
		x	x	

1. all sides equal $\rightarrow$ some sides equal;
2. all angles equal $\rightarrow$ some sides equal, has right angle;
3. has right angle, all sides equal $\rightarrow$ all angles equal.

Identities

Operations Φ:

binary: $f^{(2)}$ or $*$

unary: $f^{(1)}$ or $-$

nullary: $f^{(0)}$ or a

Variables X:

x, y, z

Terms $T_\Phi(X)$

Terms construction:

- $X \subseteq T_\Phi(X)$;
- $p_1, \ldots p_n \in T_\Phi(X)$ and $f^{(n)} \Rightarrow f^{(n)}(p_1, \ldots p_n) \in T_\Phi(X)$.

Identity

Identity is a pair (p, q), $p, q \in T_\Phi(X)$, written $p \equiv q$.

Size of Identity

Size of identity $p_1 \equiv p_2$

$$\begin{array}{l} v(p_i) \\ o(p_i) \end{array} \text{ number of occurrences of } \begin{array}{r} \text{variables} \\ \text{operations} \end{array} \text{ in } p_i.$$

Size: $l(p_1 \equiv p_2) = \sum_{i=1}^{2} v(p_i) + o(p_i)$.

Example ($x * y \equiv y * x$)

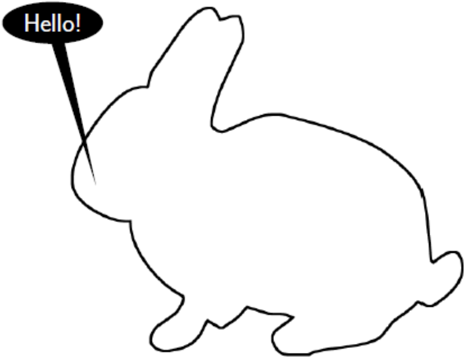
$v(x * y) = 2,$ $v(y * x) = 2,$

$o(x * y) = 1,$ $o(y * x) = 1,$

$$l(x * y \equiv y * x) = 2 + 1 + 2 + 1 = 6.$$

It is necessary to limit the size.

BUNny



BUNny

B	U	N	n	y
i	n	u		
n	a	l		
a	r	l		
r	y	a		
y		r		
		y		

Example (A bunny of size 2)

$\mathfrak{B}_5 = (\{0,1\}, (*, -, 0))$

*	0	1
0	0	0
1	1	0

-	0	1
	0	0

Definition (BUNny)

A set and a family of a binary, a unary, and a nullary operations are called a bunny.

Equivalent Identities

Satisfaction

$p^{(n)}(\bar{x}) \equiv q^{(n)}(\bar{x})$ is satisfied in $(A, (f^{(2)}, f^{(1)}, f^{(0)}))$ iff $p^{(n)}(\bar{a}) = q^{(n)}(\bar{a})$ for all $\bar{a} \in A^n$.

Equivalent Identities

Satisfaction

$p^{(n)}(\bar{x}) \equiv q^{(n)}(\bar{x})$ is satisfied in $(A, (f^{(2)}, f^{(1)}, f^{(0)}))$ iff $p^{(n)}(\bar{a}) = q^{(n)}(\bar{a})$ for all $\bar{a} \in A^n$.

Equivalent identities $p_1 \equiv p_2 \iff q_1 \equiv q_2$

Identities are equivalent iff they are satisfied in the same bunnies.

Examples

- $a \equiv a \iff x \equiv x$,

Equivalent Identities

Satisfaction

$p^{(n)}(\bar{x}) \equiv q^{(n)}(\bar{x})$ is satisfied in $(A, (f^{(2)}, f^{(1)}, f^{(0)}))$ iff $p^{(n)}(\bar{a}) = q^{(n)}(\bar{a})$ for all $\bar{a} \in A^n$.

Equivalent identities $p_1 \equiv p_2 \iff q_1 \equiv q_2$

Identities are equivalent iff they are satisfied in the same bunnies.

Examples

- $a \equiv a \iff x \equiv x$,
- $x \equiv y \iff x \equiv a$,

Equivalent Identities

Satisfaction

$p^{(n)}(\bar{x}) \equiv q^{(n)}(\bar{x})$ is satisfied in $(A, (f^{(2)}, f^{(1)}, f^{(0)}))$ iff $p^{(n)}(\bar{a}) = q^{(n)}(\bar{a})$ for all $\bar{a} \in A^n$.

Equivalent identities $p_1 \equiv p_2 \iff q_1 \equiv q_2$

Identities are equivalent iff they are satisfied in the same bunnies.

Examples

- $a \equiv a \iff x \equiv x$,
- $x \equiv y \iff x \equiv a$,
- $x \equiv a \iff x \equiv -y$.

It makes sense to avoid equivalent identities.

Motivation

Definition (Equational Class)

A class of algebras satisfying given identities.

Example (Semigroup)

The equational class of algebras with only a binary operation satisfying

$$x * (y * z) \equiv (x * y) * z;$$

Motivation

Definition (Equational Class)

A class of algebras satisfying given identities.

Example (Group)

The equational class of algebras with a binary, a unary, and a nullary operations satisfying

$$x * (y * z) \equiv (x * y) * z;$$
$$x * 1 \equiv 1 * x \equiv x;$$
$$x * (-x) \equiv (-x) * x \equiv 1;$$

Motivation

Definition (Equational Class)

A class of algebras satisfying given identities.

Example (Abelian Group)

The equational class of algebras with a binary, a unary, and a nullary operations satisfying

$$x * (y * z) \equiv (x * y) * z;$$
$$x * 1 \equiv 1 * x \equiv x;$$
$$x * (-x) \equiv (-x) * x \equiv 1;$$
$$x * y \equiv y * x.$$

Motivation

Definition (Equational Class)

A class of algebras satisfying given identities.

Definition (Variety)

A class of algebras closed under homomorphisms, subalgebras, products.

Theorem (HSP, Birkhoff 1935)

$$\textit{Variety} \quad \sim \quad \textit{equational class.}$$

Problem Statement

Problem statement

Automatic construction of the implicative theory of algebraic identities of size up to 5 (70 pairwise non-equivalent).

Related research

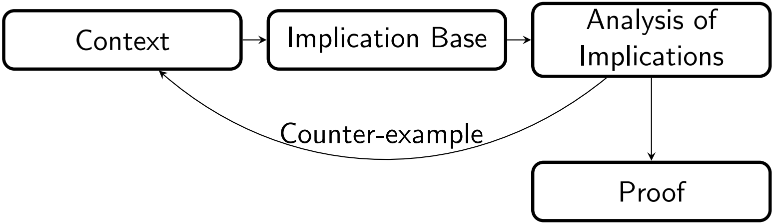
Concerning:

- Decidability of equational theories [Per67], [Tay79];
- Finding (finite) bases [BS81].

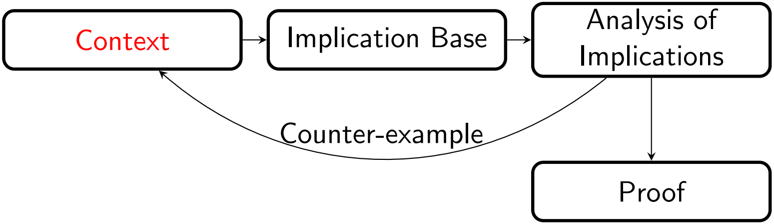
Closely related work

PhD thesis, most of research by hand [Kes13].

Attribute Exploration of Equational Classes

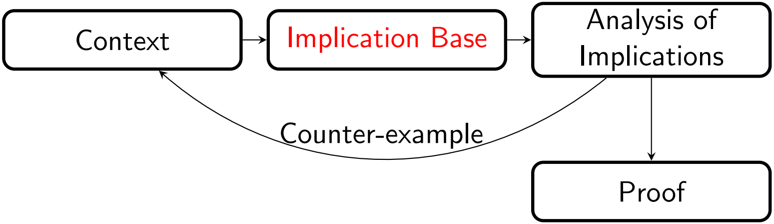


Attribute Exploration of Equational Classes



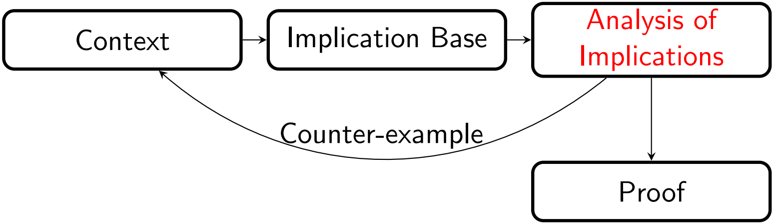
- On the first step initial (small) context is generated;
- On every step unnecessary objects are eliminated.

Attribute Exploration of Equational Classes



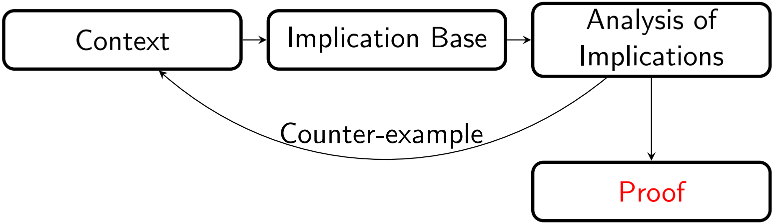
- Canonical base.

Attribute Exploration of Equational Classes



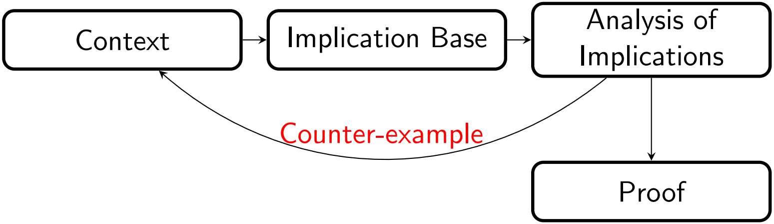
- Try to prove;
- Try to find a counter-example.

Attribute Exploration of Equational Classes



- Prover9 (from `http://www.cs.unm.edu/~mccune/mace4/`).

Attribute Exploration of Equational Classes



- Mace4 (from `http://www.cs.unm.edu/~mccune/mace4/`);
- `find_infinite_algebra`.

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \rightarrow \ x \equiv -(a * x)$.

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \rightarrow \ x \equiv -(a * x)$.

Counter-example: algebra $\mathcal{A}_\infty = (\mathbb{N}_0, (*_\infty, -_\infty, a_\infty))$

$$m *_\infty n = \begin{cases} n, & \text{if } m = 0 \text{ and } n \leq 2; \\ n -_{\mathbb{N}_0} 1, & \text{if } m = 0 \text{ and } n \geq 3; \\ 0, & \text{if } m \geq 1. \end{cases}$$

$$-_\infty n = \begin{cases} n, & \text{if } n \leq 2; \\ n + 1, & \text{if } n \geq 3. \end{cases}$$

$$a_\infty = 0.$$

Try $x = 3$.

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \rightarrow \; x \equiv -(a * x)$.

Counter-example: algebra $\mathcal{A}_\infty = (\mathbb{N}_0, (*_\infty, -_\infty, a_\infty))$

$$m *_\infty n = \begin{cases} n, & \text{if } m = 0 \text{ and } n \leq 2; \\ n -_{\mathbb{N}_0} 1, & \text{if } m = 0 \text{ and } n \geq 3; \\ 0, & \text{if } m \geq 1. \end{cases}$$

$$-_\infty n = \begin{cases} n, & \text{if } n \leq 2; \\ n + 1, & \text{if } n \geq 3. \end{cases}$$

$$a_\infty = 0.$$

$$3 \equiv a * (-3) \quad \rightarrow \quad 3 \equiv -(a * 3).$$

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \rightarrow \ x \equiv -(a * x)$.

Counter-example: algebra $\mathcal{A}_\infty = (\mathbb{N}_0, (*_\infty, -_\infty, a_\infty))$

$$m *_\infty n = \begin{cases} n, & \text{if } m = 0 \text{ and } n \leq 2; \\ n -_{\mathbb{N}_0} 1, & \text{if } m = 0 \text{ and } n \geq 3; \\ 0, & \text{if } m \geq 1. \end{cases}$$

$$-_\infty n = \begin{cases} n, & \text{if } n \leq 2; \\ n + 1, & \text{if } n \geq 3. \end{cases}$$

$$a_\infty = 0.$$

$$3 \equiv 0 * (-3) \quad \rightarrow \quad 3 \equiv -(0 * 3).$$

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \to \ x \equiv -(a * x)$.

Counter-example: algebra $\mathcal{A}_\infty = (\mathbb{N}_0, (*_\infty, -_\infty, a_\infty))$

$$m *_\infty n = \begin{cases} n, & \text{if } m = 0 \text{ and } n \leq 2; \\ n -_{\mathbb{N}_0} 1, & \text{if } m = 0 \text{ and } n \geq 3; \\ 0, & \text{if } m \geq 1. \end{cases}$$

$$-_\infty n = \begin{cases} n, & \text{if } n \leq 2; \\ n + 1, & \text{if } n \geq 3. \end{cases}$$

$$a_\infty = 0.$$

$$3 \equiv 0 * 4 \quad \to \quad 3 \equiv -2.$$

Only finite bunnies?

Lemma ([Kes13])

For finite bunnies is satisfied: $\{x \equiv a * (-x)\} \to \ x \equiv -(a * x)$.

Counter-example: algebra $\mathcal{A}_\infty = (\mathbb{N}_0, (*_\infty, -_\infty, a_\infty))$

$$m *_\infty n = \begin{cases} n, & \text{if } m = 0 \text{ and } n \leq 2; \\ n -_{\mathbb{N}_0} 1, & \text{if } m = 0 \text{ and } n \geq 3; \\ 0, & \text{if } m \geq 1. \end{cases}$$

$$-_\infty n = \begin{cases} n, & \text{if } n \leq 2; \\ n + 1, & \text{if } n \geq 3. \end{cases}$$

$$a_\infty = 0.$$

$$3 \equiv 3 \quad \to \quad 3 \not\equiv 2.$$

Template

Simplified infinite bunny template

$$\mathfrak{B}_{inf} = (\mathbb{N}, (*, -, 0))$$

*	0	1	...
0	$\mathbb{N}_{\leq 3}$	$\mathbb{N}_{\leq 3}$	$case_3$
1	$\mathbb{N}_{\leq 3}$	$\mathbb{N}_{\leq 3}$	$case_4$
...	$case_1$	$case_2$	$case_5$

$case_i(x, y) = c_{i1} \times x + c_{i2} \times y + c_{i3}$, $c_{ij} \in [-3, 3]$

-	0	1	...
	$\mathbb{N}_{\leq 3}$	$\mathbb{N}_{\leq 3}$	$case$

$case(x) = d_1 \times x + d_2$, $d_i \in [-3, 3]$

Algorithm 1: find_infinite_algebra

Input: $P_{\text{ids}} \rightarrow C_{\text{id}}$, where $P_{\text{ids}} \subseteq M_{\text{id}}$, $C_{\text{id}} \in M_{\text{id}}$.
Output: Algebra $\mathcal{A} = (\mathcal{N}_0, (*, -, 0))$ satisfying all P_{ids} and not satisfying C_{id}.

while *True* **do**
    for *id* **in** P_{ids} **do**
        sat, term = check_identity($\mathcal{A}$, id)
        if *sat = False* **then**
            backtrack($\mathcal{A}$)
            break
        if *sat = None* **then**
            update($\mathcal{A}$, term)
            break
    else
        sat, term = check_identity($\mathcal{A}$, C_{id})
        if *sat = True* **then**
            backtrack($\mathcal{A}$)
            continue
        if *sat = None* **then**
            update($\mathcal{A}$, term)
            continue
        if *sat = False* **then**
            return $\mathcal{A}$

Results

Total number of bunnies found during exploration	27266
Number of finite bunnies	626
Number of infinite bunnies	1529
Number of (unit) implications	4398
Time taken	$\simeq$78 hours

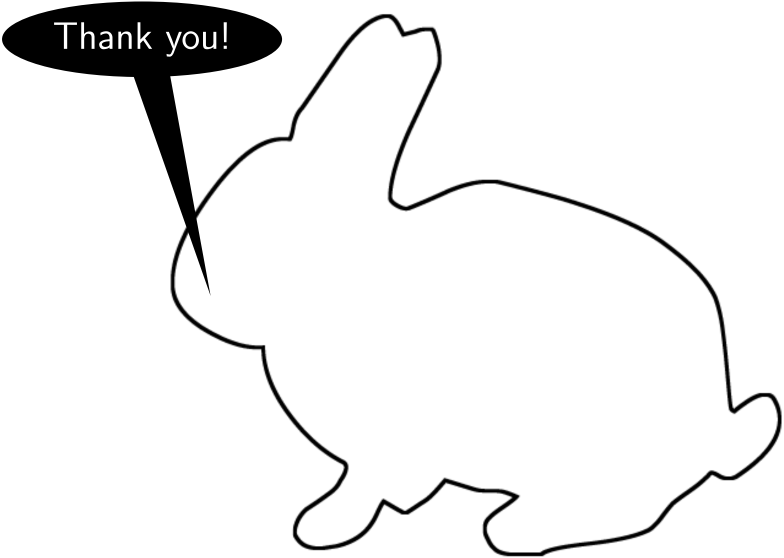
Conclusion

Conclusion

- Attribute exploration yields automatic procedure for accomplishing implication theory of equational classes;
- Introduced template suffices for considered identities.

Future work

- Can automatic Attribute Exploration be used in other domains?
- How is it possible to extend the template for bigger identities?



https://github.com/artreven

S. Burris and H.P. Sankappanavar.
A course in universal algebra, volume 78.
Springer-Verlag New York, 1981.

P. Kestler.
Strukturelle Untersuchungen eines Varietätenverbandes von Gruppoiden mit unärer Operation und ausgezeichnetem Element.
PhD thesis, TU Bergakademie, Freiberg, 2013.

P. Perkins.
Unsolvable problems for equational theories.
Notre Dame Journal of Formal Logic, 8(3):175–185, 1967.

W. Taylor.
Equational logic.
University of Houston, Department of Mathematics, 1979.