An Easy Test For Congruence Modularity

T. Dent, K. Kearnes, Á. Szendrei

2/28/11

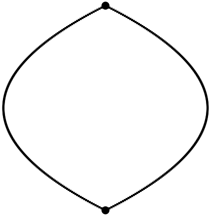
CU Logic Seminar

Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:

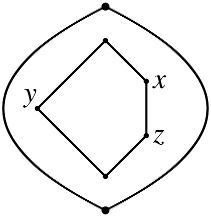
Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:



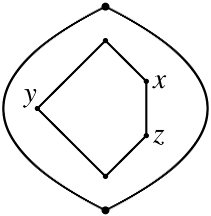
Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:



Modular lattices

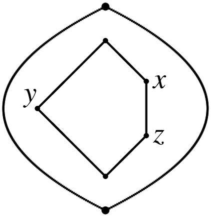
A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:



Else is *modular*.

Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:

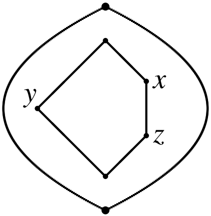


Else is *modular*. Modularity is expressed by the law

$$x \wedge (y \vee (x \wedge z)) \approx (x \wedge y) \vee (x \wedge z).$$

Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:



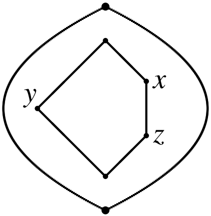
Else is *modular*. Modularity is expressed by the law

$$x \wedge (y \vee (x \wedge z)) \approx (x \wedge y) \vee (x \wedge z).$$

The modular law was discovered by Richard Dedekind as a law satisfied by the subgroup lattice of $\langle \mathbb{C}; +, -, 0 \rangle$.

Modular lattices

A lattice is *nonmodular* if it has a sublattice isomorphic to the pentagon:



Else is *modular*. Modularity is expressed by the law

$$x \wedge (y \vee (x \wedge z)) \approx (x \wedge y) \vee (x \wedge z).$$

The modular law was discovered by Richard Dedekind as a law satisfied by the subgroup lattice of $\langle \mathbb{C}; +, -, 0 \rangle$. He also proved that any law in at most 3 variables satisfied by the subgroup lattice of $\mathbb{C}$ is a consequence of the modular law.

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties.

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties. This theory has been applied to problems about counting models,

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties. This theory has been applied to problems about counting models, decidability problems,

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties. This theory has been applied to problems about counting models, decidability problems, the study of categorical algebraic properties of varieties,

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties. This theory has been applied to problems about counting models, decidability problems, the study of categorical algebraic properties of varieties, finite basis questions,

Congruence modularity

A class of algebras is congruence modular if all congruence lattices are modular.

Examples. Any class of algebras *realizing* the laws of groups or lattices is congruence modular: groups, rings, modules, lattices, Boolean algebras, etc.

Starting in the 1970's, commutator theory was developed for congruence modular varieties. This theory has been applied to problems about counting models, decidability problems, the study of categorical algebraic properties of varieties, finite basis questions, equational completeness, and more.

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$;

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$;

(b) $m_i(x,u,u,x) \approx x$ *for all* i;

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$;

(b) $m_i(x,u,u,x) \approx x$ *for all* i;

(c) $m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y)$ *for odd* i; *and*

Day's Theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$*;*

(b) $m_i(x,u,u,x) \approx x$ *for all i;*

(c) $m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y)$ *for odd i; and*

(d) $m_i(x,x,y,y) \approx m_{i+1}(x,x,y,y)$ *for even i.*

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$;

(b) $m_i(x,u,u,x) \approx x$ *for all* i;

(c) $m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y)$ *for odd* i; *and*

(d) $m_i(x,x,y,y) \approx m_{i+1}(x,x,y,y)$ *for even* i.

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$*;*

(b) $m_i(x,u,u,x) \approx x$ *for all i;*

(c) $m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y)$ *for odd i; and*

(d) $m_i(x,x,y,y) \approx m_{i+1}(x,x,y,y)$ *for even i.*

For groups, can take

Day's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $m_0(x,u,v,y) \approx x$ *and* $m_n(x,u,v,y) \approx y$*;*

(b) $m_i(x,u,u,x) \approx x$ *for all* i*;*

(c) $m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y)$ *for odd* i*; and*

(d) $m_i(x,x,y,y) \approx m_{i+1}(x,x,y,y)$ *for even* i*.*

For groups, can take

$$m_0(x,u,v,y) = x, \quad m_1(x,u,v,y) = xv^{-1}ux^{-1}y, \quad m_2(x,u,v,y) = y.$$

Gumm's Theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes the following identities for some n:

Gumm's Theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x, z, z) \approx x$ *and* $p(x, x, z) \approx z$;

Gumm's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ *for all* i;

Gumm's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ *for all* i;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd* i; *and*

Gumm's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$*;*

(b) $q_i(x,z,x) \approx x$ *for all i;*

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd i; and*

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ *for even i; and*

Gumm's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ *for all* i;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd* i; *and*

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ *for even* i; *and*

(e) $q_n(x,z,z) \approx p(x,z,z)$.

Gumm's Theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ *for all* i;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd* i; *and*

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ *for even* i; *and*

(e) $q_n(x,z,z) \approx p(x,z,z)$.

Gumm's Theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$*;*

(b) $q_i(x,z,x) \approx x$ *for all i;*

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd i; and*

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ *for even i; and*

(e) $q_n(x,z,z) \approx p(x,z,z)$.

For groups, can take

Gumm's Theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes the following identities for some n:

(a) $q_1(x,z,z) \approx x$ *and* $p(x,x,z) \approx z$;
(b) $q_i(x,z,x) \approx x$ *for all* i;
(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ *for odd* i*; and*
(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ *for even* i*; and*
(e) $q_n(x,z,z) \approx p(x,z,z)$.

For groups, can take

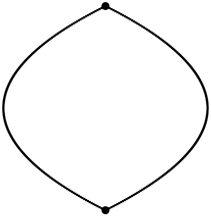
$$q_1(x,y,z) = x, \quad p(x,y,z) = xy^{-1}z$$

Modularity versus *p*-modularity

A lattice FAILS to be *p-modular* if it has a sublattice isomorphic to this one:

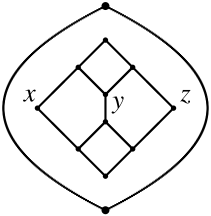
Modularity versus p-modularity

A lattice FAILS to be *p-modular* if it has a sublattice isomorphic to this one:



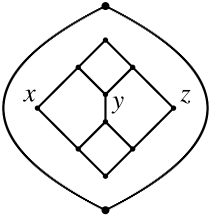
Modularity versus p-modularity

A lattice FAILS to be *p-modular* if it has a sublattice isomorphic to this one:



Modularity versus p-modularity

A lattice FAILS to be *p-modular* if it has a sublattice isomorphic to this one:



Else IS *p-modular*. p-modularity is expressed by

$$(x \vee (y \wedge z)) \wedge (z \vee (y \wedge x)) \approx (z \wedge (x \vee (y \wedge z))) \vee (x \wedge (z \vee (y \wedge x))).$$

Gedeonova's Theorem

Theorem

A variety $\mathcal{V}$ is congruence p-modular iff it realizes the following identities for some n:

Gedeonova's Theorem

Theorem

A variety $\mathcal{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$*;*

Gedeonova's Theorem

Theorem

A variety $\mathcal{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$*;*

(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ *for all i;*

Gedeonova's Theorem

Theorem

A variety $\mathscr{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$*;*

(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ *for all i;*

(c) $g_i(x,s,x,y,s,y) \approx g_{i+1}(x,s,x,y,s,y)$ *for odd i; and*

Gedeonova's Theorem

Theorem

A variety $\mathscr{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$;

(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ *for all i;*

(c) $g_i(x,s,x,y,s,y) \approx g_{i+1}(x,s,x,y,s,y)$ *for odd i; and*

(d) $g_i(x,x,s,s,y,y) \approx g_{i+1}(x,x,s,s,y,y)$ *for even i.*

Gedeonova's Theorem

Theorem

A variety $\mathscr{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x, s, t, u, v, y) \approx x$ *and* $g_n(x, s, t, u, v, y) \approx y$*;*

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ *for all i;*

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ *for odd i; and*

(d) $g_i(x, x, s, s, y, y) \approx g_{i+1}(x, x, s, s, y, y)$ *for even i.*

Gedeonova's Theorem

Theorem

A variety $\mathscr{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$*;*
(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ *for all i;*
(c) $g_i(x,s,x,y,s,y) \approx g_{i+1}(x,s,x,y,s,y)$ *for odd i; and*
(d) $g_i(x,x,s,s,y,y) \approx g_{i+1}(x,x,s,s,y,y)$ *for even i.*

Question. Is congruence p-modularity equivalent to congruence modularity for varieties?

Gedeonova's Theorem

Theorem

A variety $\mathscr{V}$ is congruence p-modular iff it realizes the following identities for some n:

(a) $g_0(x, s, t, u, v, y) \approx x$ *and* $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ *for all i;*

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ *for odd i; and*

(d) $g_i(x, x, s, s, y, y) \approx g_{i+1}(x, x, s, s, y, y)$ *for even i.*

Question. Is congruence p-modularity equivalent to congruence modularity for varieties? Yes. (Alan Day.)

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture. A variety $\mathcal{V}$ has the property that all of its topological algebras satisfy $T_0 \Rightarrow T_2$ iff

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture. A variety $\mathcal{V}$ has the property that all of its topological algebras satisfy $T_0 \Rightarrow T_2$ iff

(1) all of its topological algebras satisfy $T_0 \Rightarrow T_1$ and

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture. A variety $\mathcal{V}$ has the property that all of its topological algebras satisfy $T_0 \Rightarrow T_2$ iff

(1) all of its topological algebras satisfy $T_0 \Rightarrow T_1$ and

(2) $\mathcal{V}$ is congruence modular.

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture. A variety $\mathcal{V}$ has the property that all of its topological algebras satisfy $T_0 \Rightarrow T_2$ iff

(1) all of its topological algebras satisfy $T_0 \Rightarrow T_1$ and

(2) $\mathcal{V}$ is congruence modular.

The Congruence Modularity Conjecture

If $\mathbf{A} = \langle A; \mathcal{F} \rangle$ is an algebra, then a topology on $\mathbf{A}$ is *compatible* if all operations of $\mathbf{A}$ are continuous with respect to this topology.

If $\mathcal{V}$ is a variety, a topological algebra associated to $\mathcal{V}$ is any algebra of $\mathcal{V}$ equipped with a compatible topology.

The Congruence Modularity Conjecture. A variety $\mathcal{V}$ has the property that all of its topological algebras satisfy $T_0 \Rightarrow T_2$ iff

(1) all of its topological algebras satisfy $T_0 \Rightarrow T_1$ and

(2) $\mathcal{V}$ is congruence modular.

"If" proved by Kearnes & Sequeira; "only if" still open.

Bentz's question

Bentz's question

Bentz suggested a possible counterexample to "only if".

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$.

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$. These are the Gumm identities for congruence modularity for $n = 2$ *minus* the Gumm identity $q_1(x,y,x) \approx x$.

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$. These are the Gumm identities for congruence modularity for $n = 2$ *minus* the Gumm identity $q_1(x,y,x) \approx x$.

Question. Do the Gumm identities for $n = 2$ imply congruence modularity if you delete the Gumm identity $q_1(x,y,x) \approx x$?

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$. These are the Gumm identities for congruence modularity for $n = 2$ *minus* the Gumm identity $q_1(x,y,x) \approx x$.

Question. Do the Gumm identities for $n = 2$ imply congruence modularity if you delete the Gumm identity $q_1(x,y,x) \approx x$?

Yes.

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$. These are the Gumm identities for congruence modularity for $n = 2$ *minus* the Gumm identity $q_1(x,y,x) \approx x$.

Question. Do the Gumm identities for $n = 2$ imply congruence modularity if you delete the Gumm identity $q_1(x,y,x) \approx x$?

Yes. Any variety realizing such identities also realizes Gumm identities for $n = 30$. (Kearnes & Sequeira)

Bentz's question

Bentz suggested a possible counterexample to "only if". He showed that if you define a variety with identities guaranteeing $T_0 \Rightarrow T_1$ and add to those $x \approx q_1(x,y,y)$, $q_1(x,x,y) \approx q_2(x,x,y)$, $q_2(x,y,x) \approx x$, $q_2(x,y,y) \approx p(x,y,y)$, and $p(x,x,y) \approx y$, then topological algebras must satisfy $T_0 \Rightarrow T_2$. These are the Gumm identities for congruence modularity for $n = 2$ *minus* the Gumm identity $q_1(x,y,x) \approx x$.

Question. Do the Gumm identities for $n = 2$ imply congruence modularity if you delete the Gumm identity $q_1(x,y,x) \approx x$?

Yes. Any variety realizing such identities also realizes Gumm identities for $n = 30$. (Kearnes & Sequeira)

Cube terms

Cube terms

If $\Sigma \models F(y, \bar{z}) \approx x$ where the variables $xy\bar{z}$ are not necessarily distinct, except that $x \neq y$, then call F *weakly independent* of its first place relative to Σ.

Cube terms

If $\Sigma \models F(y, \bar{z}) \approx x$ where the variables $xy\bar{z}$ are not necessarily distinct, except that $x \neq y$, then call F *weakly independent* of its first place relative to Σ.

A *cube term* for a variety $\mathcal{V}$ is a term $C(x_1, \ldots, x_n)$ such that C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Cube terms

If $\Sigma \models F(y, \bar{z}) \approx x$ where the variables $xy\bar{z}$ are not necessarily distinct, except that $x \neq y$, then call F *weakly independent* of its first place relative to Σ.

A *cube term* for a variety $\mathcal{V}$ is a term $C(x_1, \ldots, x_n)$ such that C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Berman, Idziak, Markovic, McKenzie, Valeriote and Willard proved that any variety with a cube term is congruence modular.

Cube terms

If $\Sigma \models F(y, \bar{z}) \approx x$ where the variables $xy\bar{z}$ are not necessarily distinct, except that $x \neq y$, then call F *weakly independent* of its first place relative to Σ.

A *cube term* for a variety $\mathcal{V}$ is a term $C(x_1, \ldots, x_n)$ such that C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Berman, Idziak, Markovic, McKenzie, Valeriote and Willard proved that any variety with a cube term is congruence modular. The proof is a difficult analysis spanning 5 1/2 journal pages.

Independence versus weak independence

Let Σ be a set of identities.

Independence versus weak independence

Let Σ be a set of identities.
If $\Sigma \models F(x, x, \ldots, x) \approx x$ for each function symbol F appearing in Σ, then call Σ *idempotent*.

Independence versus weak independence

Let Σ be a set of identities.
If $\Sigma \models F(x, x, \ldots, x) \approx x$ for each function symbol F appearing in Σ, then call Σ *idempotent*.

If $\Sigma \models F(x, \bar{z}) \approx F(y, \bar{z})$ where all variables in the string $xy\bar{z}$ are distinct, then call F *independent* of its first place.

Independence versus weak independence

Let Σ be a set of identities.
If $\Sigma \models F(x, x, \ldots, x) \approx x$ for each function symbol F appearing in Σ, then call Σ *idempotent*.

If $\Sigma \models F(x, \bar{z}) \approx F(y, \bar{z})$ where all variables in the string $xy\bar{z}$ are distinct, then call F *independent* of its first place.

Note: If Σ is idempotent and F is independent of its first place, then

$$\Sigma \models F(y, x, \ldots, x) \approx F(x, x, \ldots, x) \approx x,$$

so F is weakly independent of its first place.

The derivative of a set of identities

Let Σ be an idempotent set of identities. Let $\mathcal{W}$ be the set of pairs (F, i), where F is a function symbol in Σ and i is a place of F, such that Σ proves F is weakly independent of its ith place.

The derivative of a set of identities

Let Σ be an idempotent set of identities. Let $\mathcal{W}$ be the set of pairs (F, i), where F is a function symbol in Σ and i is a place of F, such that Σ proves F is weakly independent of its ith place.

The *derivative* of Σ is the set Σ' obtained from Σ by adding identities expressing that F is independent of its ith place for each $(F, i) \in \mathcal{W}$.

The derivative of a set of identities

Let Σ be an idempotent set of identities. Let $\mathcal{W}$ be the set of pairs (F, i), where F is a function symbol in Σ and i is a place of F, such that Σ proves F is weakly independent of its ith place.

The *derivative* of Σ is the set Σ' obtained from Σ by adding identities expressing that F is independent of its ith place for each $(F, i) \in \mathcal{W}$.

Example. If $\Sigma = \{F(x, y, y) \approx x\}$, then

$$\Sigma' = \{F(x, y, y) \approx x, F(x, y, z) \approx F(x, y', z), F(x, y, z) \approx F(x, y, z')\}$$

where $xyy'zz'$ are all distinct.

Main theorem

Theorem

A variety $\mathscr{V}$ is congruence modular iff it realizes some set Σ of idempotent identities where Σ' is inconsistent.

Main theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes some set Σ of idempotent identities where Σ' is inconsistent.

Main theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes some set Σ of idempotent identities where Σ' is inconsistent.

Easy direction: take Σ to be a set of Day identities.

Main theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes some set Σ of idempotent identities where Σ' is inconsistent.

Easy direction: take Σ to be a set of Day identities.

From identity (b), $\Sigma \models m_i(x, y, y, x) \approx x$, infer $\Sigma \models m_i(x, x, x, x) \approx x$, so Σ is a set of idempotent identities. Also infer that each m_i is weakly independent of its middle places.

Main theorem

Theorem

A variety $\mathcal{V}$ is congruence modular iff it realizes some set Σ of idempotent identities where Σ' is inconsistent.

Easy direction: take Σ to be a set of Day identities.

From identity (b), $\Sigma \models m_i(x,y,y,x) \approx x$, infer $\Sigma \models m_i(x,x,x,x) \approx x$, so Σ is a set of idempotent identities. Also infer that each m_i is weakly independent of its middle places.

From identities (a), (c) and (d), infer

$$\Sigma' \models x \overset{(a)}{\approx} m_0(x,*,*,y) \overset{(d)}{\approx} m_1(x,*,*,y) \overset{(c)}{\approx} \cdots \overset{(?)}{\approx} m_n(x,*,*,y) \overset{(a)}{\approx} y.$$

Application I. Gedeonova's problem.

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ for all i;

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ for all i;

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ for odd i; and

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ for all i;

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ for odd i; and

(d) $g_i(x, x, s, s, y, y) \approx g_{i+1}(x, x, s, s, y, y)$ for even i.

Application I. Gedeonova's problem.

(a) $g_0(x,s,t,u,v,y) \approx x$ and $g_n(x,s,t,u,v,y) \approx y$;
(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ for all i;
(c) $g_i(x,s,x,y,s,y) \approx g_{i+1}(x,s,x,y,s,y)$ for odd i; and
(d) $g_i(x,x,s,s,y,y) \approx g_{i+1}(x,x,s,s,y,y)$ for even i.

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ for all i;

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ for odd i; and

(d) $g_i(x, x, s, s, y, y) \approx g_{i+1}(x, x, s, s, y, y)$ for even i.

From identity (b) infer that (i) Σ is idempotent and (ii) each g_i is weakly independent of its four middle places.

Application I. Gedeonova's problem.

(a) $g_0(x, s, t, u, v, y) \approx x$ and $g_n(x, s, t, u, v, y) \approx y$;

(b) $g_i(x, x, y, y, x, x) \approx g_i(x, y, x, x, y, x) \approx x$ for all i;

(c) $g_i(x, s, x, y, s, y) \approx g_{i+1}(x, s, x, y, s, y)$ for odd i; and

(d) $g_i(x, x, s, s, y, y) \approx g_{i+1}(x, x, s, s, y, y)$ for even i.

From identity (b) infer that (i) Σ is idempotent and (ii) each g_i is weakly independent of its four middle places.

From identities (a), (c) and (d), infer

$$\Sigma' \models x \overset{\text{(a)}}{\approx} g_0(x, *, *, *, *, y) \overset{\text{(d)}}{\approx} g_1(x, *, *, *, *, y) \overset{\text{(c)}}{\approx} \cdots \overset{\text{(?)}}{\approx} g_n(x, *, *, *, *, y) \overset{\text{(a)}}{\approx} y.$$

Application II. Bentz's question.

Application II. Bentz's question.

(a) $q_1(x, z, z) \approx x$ and $p(x, x, z) \approx z$;

Application II. Bentz's question.

(a) $q_1(x, z, z) \approx x$ and $p(x, x, z) \approx z$;

(b) $q_i(x, z, x) \approx x$ for all $i \neq 1$;

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

From identities (a) and (b) infer that Σ is idempotent.

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

From identities (a) and (b) infer that Σ is idempotent. From (b) infer that each q_i is weakly independent of its middle place, except possibly q_1.

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

From identities (a) and (b) infer that Σ is idempotent. From (b) infer that each q_i is weakly independent of its middle place, except possibly q_1. From (a) infer this for q_1 and for p.

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

From identities (a) and (b) infer that Σ is idempotent. From (b) infer that each q_i is weakly independent of its middle place, except possibly q_1. From (a) infer this for q_1 and for p.

Altogether,

$$\Sigma' \models x \approx q_1(x,*,z) \approx q_2(x,*,z) \approx \cdots \approx q_n(x,*,z) \approx p(x,*,z) \approx z.$$

Application II. Bentz's question.

(a) $q_1(x,z,z) \approx x$ and $p(x,x,z) \approx z$;

(b) $q_i(x,z,x) \approx x$ for all $i \neq 1$;

(c) $q_i(x,x,z) \approx q_{i+1}(x,x,z)$ for odd i; and

(d) $q_i(x,z,z) \approx q_{i+1}(x,z,z)$ for even i; and

(e) $q_n(x,z,z) \approx p(x,z,z)$.

From identities (a) and (b) infer that Σ is idempotent. From (b) infer that each q_i is weakly independent of its middle place, except possibly q_1. From (a) infer this for q_1 and for p.

Altogether,

$$\Sigma' \models x \approx q_1(x,*,z) \approx q_2(x,*,z) \approx \cdots \approx q_n(x,*,z) \approx p(x,*,z) \approx z.$$

Note: This shows that Gumm's identities are slightly redundant.

Application III. Cube terms.

Application III. Cube terms.

Recall: $C(x_1, \ldots, x_n)$ is a cube term for $\mathcal{V}$ if C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Application III. Cube terms.

Recall: $C(x_1, \ldots, x_n)$ is a cube term for $\mathcal{V}$ if C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Let Σ be a set of identities of $\mathcal{V}$ asserting weak independence for each place of C.

Application III. Cube terms.

Recall: $C(x_1, \ldots, x_n)$ is a cube term for $\mathcal{V}$ if C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.

Let Σ be a set of identities of $\mathcal{V}$ asserting weak independence for each place of C.

Σ is an idempotent set of identities realized in $\mathcal{V}$, which asserts that C is weakly independent of all places.

Application III. Cube terms.

Recall: $C(x_1, \ldots, x_n)$ is a cube term for $\mathcal{V}$ if C is weakly independent of all places relative to $\mathrm{Eq}(\mathcal{V})$.
Let Σ be a set of identities of $\mathcal{V}$ asserting weak independence for each place of C.
Σ is an idempotent set of identities realized in $\mathcal{V}$, which asserts that C is weakly independent of all places.
C is fully independent of all places relative to Σ', so

$$\Sigma' \models x \approx C(x, x, \ldots, x) \approx C(y, y, \ldots, y) \approx y.$$

Postscript

After the talk, Walter Taylor wrote to me to say that George McNulty proved that “there is no algorithm that correctly states, given a finite set of equations, whether the variety defined by that set is congruence-modular”.

Postscript

After the talk, Walter Taylor wrote to me to say that George McNulty proved that “there is no algorithm that correctly states, given a finite set of equations, whether the variety defined by that set is congruence-modular”.

Walter adds “this appears in Theorem 3.15 of G. McNulty, PhD Thesis, Berkeley, 1972”.

Postscript

After the talk, Walter Taylor wrote to me to say that George McNulty proved that "there is no algorithm that correctly states, given a finite set of equations, whether the variety defined by that set is congruence-modular".

Walter adds "this appears in Theorem 3.15 of G. McNulty, PhD Thesis, Berkeley, 1972".

(This does not contradict anything in the talk.)