Affine complete permutation groups

András Pongrácz, Peter Mayr, Gábor Horváth

ELTE Budapest, Hungary

Stará Lesná, September 2009.

Definition

Affine completeness

An algebra $\mathcal{A}$ is affine complete if every compatible function is a polynomial on $\mathcal{A}$.

Definition

Affine completeness

An algebra $\mathcal{A}$ is affine complete if every compatible function is a polynomial on $\mathcal{A}$.

Definition

$f : A^k \to A$ compatible : for all $\theta \in Con(\mathcal{A})$ we have $(\mathbf{a}, \mathbf{b}) \in \theta \Rightarrow (f(\mathbf{a}), f(\mathbf{b})) \in \theta$.

Definition

Affine completeness

An algebra $\mathcal{A}$ is affine complete if every compatible function is a polynomial on $\mathcal{A}$.

Definition

$f : A^k \to A$ compatible : for all $\theta \in Con(\mathcal{A})$ we have $(\mathbf{a}, \mathbf{b}) \in \theta \Rightarrow (f(\mathbf{a}), f(\mathbf{b})) \in \theta$.

- constants, fundamental operations

Definition

Affine completeness

An algebra $\mathcal{A}$ is affine complete if every compatible function is a polynomial on $\mathcal{A}$.

Definition

$f : A^k \to A$ compatible : for all $\theta \in Con(\mathcal{A})$ we have $(\mathbf{a}, \mathbf{b}) \in \theta \Rightarrow (f(\mathbf{a}), f(\mathbf{b})) \in \theta$.

- constants, fundamental operations
- polynomials

Definition

Affine completeness

An algebra $\mathcal{A}$ is affine complete if every compatible function is a polynomial on $\mathcal{A}$.

Definition

$f : A^k \to A$ compatible : for all $\theta \in Con(\mathcal{A})$ we have $(\mathbf{a}, \mathbf{b}) \in \theta \Rightarrow (f(\mathbf{a}), f(\mathbf{b})) \in \theta$.

- constants, fundamental operations
- polynomials

k-affine completeness

An algebra $\mathcal{A}$ is k-affine coplete if every compatible function of arity at most k is a polynomial on $\mathcal{A}$.

Examples

Fields, Boolean algebras

Finite fields, 2-element Boolean algebra: every function is a polynomial.
These are affine complete.

Examples

Fields, Boolean algebras

Finite fields, 2-element Boolean algebra: every function is a polynomial. These are affine complete.

Z_p

Examples

Fields, Boolean algebras

Finite fields, 2-element Boolean algebra: every function is a polynomial. These are affine complete.

Z_p

- every function is compatible

Examples

Fields, Boolean algebras

Finite fields, 2-element Boolean algebra: every function is a polynomial.
These are affine complete.

Z_p

- every function is compatible
- polynomials: $\sum_{i=1}^{n} a_i x_i + b$

Examples

Fields, Boolean algebras

Finite fields, 2-element Boolean algebra: every function is a polynomial. These are affine complete.

Z_p

- every function is compatible
- polynomials: $\sum_{i=1}^{n} a_i x_i + b$
- $\Rightarrow$ not affine complete

Grätzer

Describe the affine complete algebras.

Grätzer

Describe the affine complete algebras.

First significant results:

Grätzer

Describe the affine complete algebras.

First significant results:

- Boolean algebras

Grätzer

Describe the affine complete algebras.

First significant results:

- Boolean algebras
- Bounded distributive lattices: not containing proper Boolean intervals

Some known results

- Abelian groups: K. Kaarli
- Semilattices: K. Kaarli, L. Márki, E. T. Schmidt
- Vector spaces: H. Werner
- Distributive lattices: M. Ploščica
- Stone algebras: M. Haviar, M. Ploščica
- Kleene algebras: M. Haviar, K. Kaarli, M. Ploščica

Definition

G-set

Definition

G-set

- (Ω, G) pair

Definition

G-set

- (Ω, G) pair
- underlying set: Ω

Definition

G-set

- (Ω, G) pair
- underlying set: Ω
- type: for all $g \in G$ a unary operation is given:

$$m_g : \alpha \mapsto g\alpha$$

Definition

G-set

- (Ω, G) pair
- underlying set: Ω
- type: for all $g \in G$ a unary operation is given:

$$m_g : \alpha \mapsto g\alpha$$

Transitive group actions

Definition

G-set

- (Ω, G) pair
- underlying set: Ω
- type: for all $g \in G$ a unary operation is given:

$$m_g : \alpha \mapsto g\alpha$$

Transitive group actions

- $S \leq G$, Ω: cosets of S

Definition

G-set

- (Ω, G) pair
- underlying set: Ω
- type: for all $g \in G$ a unary operation is given:

$$m_g : \alpha \mapsto g\alpha$$

Transitive group actions

- $S \leq G$, Ω: cosets of S
- $m_g(hS) = ghS$

Congruences

Transitive group actions

Congruences

- $S \leq H \leq G$

Transitive group actions

Congruences

- $S \leq H \leq G$

Transitive group actions

Congruences

- $S \leq H \leq G$

$$\rho_H = \{(aS, bS) \in \Omega \times \Omega | a, b \in G, aH = bH\}$$

Transitive group actions

Congruences

- $S \leq H \leq G$

$$\rho_H = \{(aS, bS) \in \Omega \times \Omega | a, b \in G, aH = bH\}$$

- Congruences $\leftrightsquigarrow \{H | S \leq H \leq G\}$

Transitive group actions

Congruences

- $S \leq H \leq G$

$$\rho_H = \{(aS, bS) \in \Omega \times \Omega | a, b \in G, aH = bH\}$$

- Congruences $\leftrightsquigarrow \{H | S \leq H \leq G\}$
- $Con((\Omega, G)) = [S, G] \leq L(G)$

Transitive group actions

Congruences

- $S \leq H \leq G$

$$\rho_H = \{(aS, bS) \in \Omega \times \Omega | a, b \in G, aH = bH\}$$

- Congruences $\leftrightsquigarrow$ $\{H | S \leq H \leq G\}$
- $Con((\Omega, G)) = [S, G] \leq L(G)$

Regular G-sets

$Con(R(G)) = \{\rho_H | H \leq G\} \cong L(G)$ (subgroup lattice)

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G
f compatible on $R(G)$: for all $H \leq G$ and $a, b \in G$

$$aH = bH \Rightarrow f(a)H = f(b)H$$

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G
f compatible on $R(G)$: for all $H \leq G$ and $a, b \in G$

$$aH = bH \Rightarrow f(a)H = f(b)H$$

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G
f compatible on $R(G)$: for all $H \leq G$ and $a, b \in G$

$$aH = bH \Rightarrow f(a)H = f(b)H$$

- constants $x \mapsto g$, $g \in G$

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G
f compatible on $R(G)$: for all $H \leq G$ and $a, b \in G$

$$aH = bH \Rightarrow f(a)H = f(b)H$$

- constants $x \mapsto g$, $g \in G$
- left translations $x \mapsto gx$, $g \in G$

Regular actions

Unary compatible functions

$R(G)$: regular permutation representation of G
f compatible on $R(G)$: for all $H \leq G$ and $a, b \in G$

$$aH = bH \Rightarrow f(a)H = f(b)H$$

- constants $x \mapsto g$, $g \in G$
- left translations $x \mapsto gx$, $g \in G$
- These are the only unary polynomial functions on $R(G)$.

1-affine completeness

Theorem

Pálfy (1984.): Classification of minimal algebras.

1-affine completeness

Theorem

Pálfy (1984.): Classification of minimal algebras.

Corollary

(Ω, G) 1-affine complete $\Rightarrow$ affine complete, except:

1-affine completeness

Theorem

Pálfy (1984.): Classification of minimal algebras.

Corollary

(Ω, G) 1-affine complete $\Rightarrow$ affine complete, except:

- $|\Omega| = 2$

1-affine completeness

Theorem

Pálfy (1984.): Classification of minimal algebras.

Corollary

(Ω, G) 1-affine complete $\Rightarrow$ affine complete, except:

- $|\Omega| = 2$
- There exists a division ring D and a vector space ${}_D V$ such that $\Omega =_D V$ and $G = \{x \mapsto dx + v | d \in D, v \in V\}$

Problem

Describe the 1-affine complete G-sets.

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.
Aim: $xH = yH \Rightarrow x^2 H = y^2 H$

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.
Aim: $xH = yH \Rightarrow x^2H = y^2H$

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.
Aim: $xH = yH \Rightarrow x^2H = y^2H$
$x^2H = xHx$

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.
Aim: $xH = yH \Rightarrow x^2H = y^2H$
$x^2H = xHx$
$x^2H = yHx$

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.

Aim: $xH = yH \Rightarrow x^2H = y^2H$

$x^2H = xHx$

$x^2H = yHx$

$x^2H = yxH$

Necessary conditions

Proposition

Let G be an abelian group. Then $R(G)$ is not 1-affine complete, except if G is an elementary abelian 2-group.

Proof

$x \mapsto x^2$ is compatible.
Aim: $xH = yH \Rightarrow x^2H = y^2H$
$x^2H = xHx$
$x^2H = yHx$
$x^2H = yxH$
$x^2H = y^2H$

Necessary conditions

Proposition

$x \mapsto x^{|G:Z(G)|}$ (transfer) is compatible
$R(G)$ is 1-affine complete $\Rightarrow |G : Z(G)|$ is divisible by $exp(G)$.

Necessary conditions

Proposition

$x \mapsto x^{|G:Z(G)|}$ (transfer) is compatible
$R(G)$ is 1-affine complete $\Rightarrow |G : Z(G)|$ is divisible by $exp(G)$.

Lemma (Typical counterexample)

$G = A \times B$, A, B are proper subgroups and $gcd(|A|, |B|) = 1$. Then $R(G)$ is not 1-affine complete.

Expanding property

Theorem

Let $A, B \leq G$ such that $\langle A, B \rangle = G$. If $R(A), R(B)$ are 1-affine complete, then exactly one of the following holds:

Expanding property

Theorem

Let $A, B \leq G$ such that $\langle A, B \rangle = G$. If $R(A), R(B)$ are 1-affine complete, then exactly one of the following holds:

- $R(G)$ is 1-affine complete

Expanding property

Theorem

Let $A, B \leq G$ such that $\langle A, B \rangle = G$. If $R(A), R(B)$ are 1-affine complete, then exactly one of the following holds:

- $R(G)$ is 1-affine complete
- $G = A \times B$ and $gcd(|A|, |B|) = 1$.

Corollary

Definition

Let $C(G) := \langle H \leq G \mid R(H)$ is $1-$ affine complete $\rangle$.

Corollary

Definition

Let $C(G) := \langle H \leq G \mid R(H) \text{ is } 1 - \text{affine complete } \rangle$.

Properties of $C(G)$

Corollary

Definition

Let $C(G) := \langle H \leq G \mid R(H) \text{ is } 1-\text{affine complete } \rangle$.

Properties of $C(G)$

- $C(G)$ char G

Corollary

Definition

Let $C(G) := \langle H \leq G \mid R(H) \text{ is } 1 - \text{affine complete } \rangle$.

Properties of $C(G)$

- $C(G)$ char G
- $C(G)$ is the direct product of 1-affine complete maximal subgroups.

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups
- Dihedral groups, S_n (for all n), A_n ($n \geq 4$), finite nonabelian simple groups

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups
- Dihedral groups, S_n (for all n), A_n ($n \geq 4$), finite nonabelian simple groups
- Groups all of whose minimal normal subgroups are nonabelian

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups
- Dihedral groups, S_n (for all n), A_n ($n \geq 4$), finite nonabelian simple groups
- Groups all of whose minimal normal subgroups are nonabelian
- $GL(n, F)$ ($n \geq 2$)

1-affine complete G-sets

Theorem: Mayr, Horváth, Szabó, Pongrácz

The regular G-set corresponding to the following groups are 1-affine complete:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups
- Dihedral groups, S_n (for all n), A_n ($n \geq 4$), finite nonabelian simple groups
- Groups all of whose minimal normal subgroups are nonabelian
- $GL(n, F)$ ($n \geq 2$)
- G arbitrary: $G \times D_n$ with $n = 2exp(G)$

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

Problems

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

Problems

- Describe 1-affine complete G-sets

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

Problems

- Describe 1-affine complete G-sets
- Describe groups without 1-affine complete subgroups, i.e.:

Problems

$C(G) = 1$

If $C(G) = 1$, then $|G|$ is odd (hence solvable) and does not contain subgroups isomorphic to:

- nonabelian p-groups of exponent p
- $Z_p \rtimes Z_q$ (nonabelian), $(Z_p)^n \rtimes Z_q$
- Frobenius groups, Zassenhaus groups

Problems

- Describe 1-affine complete G-sets
- Describe groups without 1-affine complete subgroups, i.e.:
- When is $C(G) = 1$?