Talk #5: Pálfy's Theorem

The structure of $\langle 0, 1 \rangle$-minimal algebras

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

The structure of $\langle 0,1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0,1\rangle$-minimal:

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

The structure of $\langle 0, 1 \rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1 \rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation:

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is ‘polynomially equivalent’ to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is ‘polynomially equivalent’ to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.

The structure of $\langle 0,1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0,1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

The structure of $\langle 0, 1 \rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1 \rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem.

The structure of $\langle 0,1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0,1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem. That's all.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is ‘polynomially equivalent’ to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy’s Theorem. That’s all.

Proof.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem. That's all.

Proof.
Case 1.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem. That's all.

Proof.
Case 1. If $\mathbf{A}$ is essentially unary, then it is polynomially equivalent to a G-set.

The structure of $\langle 0, 1 \rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1 \rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is ‘polynomially equivalent’ to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy’s Theorem. That’s all.

Proof.
Case 1. If $\mathbf{A}$ is essentially unary, then it is polynomially equivalent to a G-set.
□

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem. That's all.

Proof.
Case 1. If $\mathbf{A}$ is essentially unary, then it is polynomially equivalent to a G-set.
□

Remaining Case.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is ‘polynomially equivalent’ to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy’s Theorem. That’s all.

Proof.
Case 1. If $\mathbf{A}$ is essentially unary, then it is polynomially equivalent to a G-set.
□

Remaining Case. If $\mathbf{A}$ is minimal, $|A| \geq 3$, and not essentially unary, then $\mathbf{A}$ is polynomially equivalent to a vector space over a finite field.

The structure of $\langle 0, 1\rangle$-minimal algebras

I will consider only finite algebras $\mathbf{A} = \mathbf{A}_A$ that equal their full polynomial expansion. In this setting $C_1(\mathbf{A}_A) = \mathrm{Pol}_1(\mathbf{A})$.

$\mathbf{A}$ is **minimal** if it is $\langle 0, 1\rangle$-minimal: $|A| > 1$ and every $p(x) \in \mathrm{Pol}_1(\mathbf{A})$ is a permutation of A or is constant.

Observation: Any algebra that is 'polynomially equivalent' to one of the following is minimal.

1. An algebra of size 2.
2. A G-set.
3. A vector space over a finite field.

Pálfy's Theorem. That's all.

Proof.
Case 1. If $\mathbf{A}$ is essentially unary, then it is polynomially equivalent to a G-set.
□

Remaining Case. If $\mathbf{A}$ is minimal, $|A| \geq 3$, and not essentially unary, then $\mathbf{A}$ is polynomially equivalent to a vector space over a finite field. ?????

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function.

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is,

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$$p(a_1, \ldots, a_{i-i}, b, a_{i+1}, \ldots, a_n) \neq p(a_1, \ldots, a_{i-i}, c, a_{i+1}, \ldots, a_n).$$

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$$p(a_1, \ldots, a_{i-i}, b, a_{i+1}, \ldots, a_n) \neq p(a_1, \ldots, a_{i-i}, c, a_{i+1}, \ldots, a_n).$$

Given a polynomial p, a variable x_i, and an element a, let $D(a, i)$ be the set of j such that

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$$p(a_1, \ldots, a_{i-i}, b, a_{i+1}, \ldots, a_n) \neq p(a_1, \ldots, a_{i-i}, c, a_{i+1}, \ldots, a_n).$$

Given a polynomial p, a variable x_i, and an element a, let $D(a, i)$ be the set of j such that

$$p[a, i] := p(x_1, \ldots, x_{i-i}, a, x_{i+1}, \ldots, x_n)$$

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$$p(a_1, \ldots, a_{i-i}, b, a_{i+1}, \ldots, a_n) \neq p(a_1, \ldots, a_{i-i}, c, a_{i+1}, \ldots, a_n).$$

Given a polynomial p, a variable x_i, and an element a, let $D(a, i)$ be the set of j such that

$$p[a, i] := p(x_1, \ldots, x_{i-i}, a, x_{i+1}, \ldots, x_n)$$

depends on x_j.

$p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ depends on x_i.

Say that a polynomially operation $p(x_1, \ldots, x_{i-1}, x_i, x_{i+1} \ldots, x_n)$ of $\mathbf{A}$ **depends** on x_i if there exist parameters from $\mathbf{A}$ so that

$$p(a_1, \ldots, a_{i-i}, x, a_{i+1}, \ldots, a_n)$$

is a nonconstant function. That is, there exist $b \neq c$ in $\mathbf{A}$ such that

$$p(a_1, \ldots, a_{i-i}, b, a_{i+1}, \ldots, a_n) \neq p(a_1, \ldots, a_{i-i}, c, a_{i+1}, \ldots, a_n).$$

Given a polynomial p, a variable x_i, and an element a, let $D(a, i)$ be the set of j such that

$$p[a, i] := p(x_1, \ldots, x_{i-i}, a, x_{i+1}, \ldots, x_n)$$

depends on x_j. (Here $p[a, i]$ is p 'constrained' by the condition '$x_i = a$'.)

Reducing to an essentially binary polynomial

Reducing to an essentially binary polynomial

Lemma.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables,

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j,

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant,

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$. Necessarily $i \neq k \neq j$.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$. Necessarily $i \neq k \neq j$. Since $p[a, i]$ depends on k but not j,

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$. Necessarily $i \neq k \neq j$. Since $p[a, i]$ depends on k but not j, $p[a, i; b, j]$ still depends on k.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$. Necessarily $i \neq k \neq j$. Since $p[a, i]$ depends on k but not j, $p[a, i; b, j]$ still depends on k. Hence $p[b, j]$ depends on k.

Reducing to an essentially binary polynomial

Lemma. If $n \geq 2$ and $p(x_1, \ldots, x_n)$ depends on all variables, then there exist $i \neq j$ and $a, b \in A$ such that $p[a, i]$ and $p[b, j]$ depend on all remaining variables.

Proof. If p depends on x_j, then there exist parameters so that

$$p(a_1, \ldots, a_{j-i}, x, a_{j+1}, \ldots, a_n)$$

is not constant, so $j \in D(a_i, i)$ for all $i \neq j$. Thus:

Fact 1. $(\forall j \neq i)(\exists a)(j \in D(a, i))$.

Fact 2. If $i \neq j$ and $j \notin D(a, i)$, then for any b we have $D(a, i) \subseteq D(b, j)$.

For **Fact 2**, choose $k \in D(a, i)$. Necessarily $i \neq k \neq j$. Since $p[a, i]$ depends on k but not j, $p[a, i; b, j]$ still depends on k. Hence $p[b, j]$ depends on k. Hence $k \in D(b, j)$.

Reducing to an essentially binary polynomial, 2

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2.

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$,

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea —

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study:

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim.

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k,

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.)

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.)
The polynomial $p[a, i]$ depends on all remaining variables.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.)
The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim.

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a,i)$ but $k \in D(a,i)$, then for any b we have $k \in D(b,j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a,i) so that $k \in D(a,i)$ and so that the choice of (a,i) maximizes $D(a,i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a,i) with $k \in D(a,i)$ by **Fact 1**.)
The polynomial $p[a,i]$ depends on all remaining variables.

Proof of Claim. Assume not.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$,

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts,

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b, j)$ for any b (**Fact 2**).

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b, j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b, j)$ by **Fact 1**.

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a,i)$ but $k \in D(a,i)$, then for any b we have $k \in D(b,j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a,i) so that $k \in D(a,i)$ and so that the choice of (a,i) maximizes $D(a,i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a,i) with $k \in D(a,i)$ by **Fact 1**.) The polynomial $p[a,i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a,i)$. Since $k \in D(a,i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b,j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b,j)$ by **Fact 1**. (ii) $D(a,i)$ is maximal for $k \in D(a,i)$,

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b, j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b, j)$ by **Fact 1**. (ii) $D(a, i)$ is maximal for $k \in D(a, i)$, (iii) $D(a, i) \subseteq D(b, j)$ (**Fact 2**),

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a,i)$ but $k \in D(a,i)$, then for any b we have $k \in D(b,j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. $\square$

Claim. Choose and fix k, then choose (a,i) so that $k \in D(a,i)$ and so that the choice of (a,i) maximizes $D(a,i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a,i) with $k \in D(a,i)$ by **Fact 1**.) The polynomial $p[a,i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a,i)$. Since $k \in D(a,i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b,j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b,j)$ by **Fact 1**. (ii) $D(a,i)$ is maximal for $k \in D(a,i)$, (iii) $D(a,i) \subseteq D(b,j)$ (**Fact 2**), and $i \in D(b,j) \setminus D(a,i)$.

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a, i)$ but $k \in D(a, i)$, then for any b we have $k \in D(b, j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a, i) so that $k \in D(a, i)$ and so that the choice of (a, i) maximizes $D(a, i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a, i) with $k \in D(a, i)$ by **Fact 1**.) The polynomial $p[a, i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a, i)$. Since $k \in D(a, i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b, j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b, j)$ by **Fact 1**. (ii) $D(a, i)$ is maximal for $k \in D(a, i)$, (iii) $D(a, i) \subseteq D(b, j)$ (**Fact 2**), and $i \in D(b, j) \setminus D(a, i)$. This contradiction proves the **Claim.**

Reducing to an essentially binary polynomial, 2

Continuation of Proof.

Reiterating the argument for Fact 2. If i, j, k are distinct and $j \notin D(a,i)$ but $k \in D(a,i)$, then for any b we have $k \in D(b,j)$.

Underlying idea — study: $p(x_1, \ldots, \underbrace{a}_{i}, \ldots, x_j, \ldots, x_k, \ldots)$. □

Claim. Choose and fix k, then choose (a,i) so that $k \in D(a,i)$ and so that the choice of (a,i) maximizes $D(a,i)$ with respect to $\subseteq$ for this fixed k. (There will exist at least one pair (a,i) with $k \in D(a,i)$ by **Fact 1**.) The polynomial $p[a,i]$ depends on all remaining variables.

Proof of Claim. Assume not. Let $j \neq i$ be such that $j \notin D(a,i)$. Since $k \in D(a,i)$, we necessarily have $i \neq k \neq j$ $(\neq i)$. Gathering all facts, we have (i) $k \in D(b,j)$ for any b (**Fact 2**). We may choose a particular b so that $i \in D(b,j)$ by **Fact 1**. (ii) $D(a,i)$ is maximal for $k \in D(a,i)$, (iii) $D(a,i) \subseteq D(b,j)$ (**Fact 2**), and $i \in D(b,j) \setminus D(a,i)$. This contradiction proves the **Claim.** □

Reducing to an essentially binary polynomial, 3

Reducing to an essentially binary polynomial, 3

Completing the Proof.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Corollary.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Corollary. If an algebra has a polynomial that depends on n-variables,

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$,

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. □

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. □

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. □

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. $\square$

For emphasis:

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. □

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. □

For emphasis:

Corollary.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. □

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. □

For emphasis:

Corollary. Any minimal algebra $\mathbf{A}$ that is not essentially unary will have an essentially binary polynomial $q(x_1, x_2)$.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\Box$

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. $\Box$

For emphasis:

Corollary. Any minimal algebra $\mathbf{A}$ that is not essentially unary will have an essentially binary polynomial $q(x_1, x_2)$. Moreover, there will be elements $a, b \in A$ such that $q[a, 1] = q(a, y)$ and and $q[b, 2] = q(x, b)$ are permutations of A.

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\square$

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. $\square$

For emphasis:

Corollary. Any minimal algebra $\mathbf{A}$ that is not essentially unary will have an essentially binary polynomial $q(x_1, x_2)$. Moreover, there will be elements $a, b \in A$ such that $q[a, 1] = q(a, y)$ and and $q[b, 2] = q(x, b)$ are permutations of A.

I will call such a binary polynomial a "q-polynomial",

Reducing to an essentially binary polynomial, 3

Completing the Proof.

We have shown that for any k there is a pair (a, i) with $i \neq k$ such that $p[a, i]$ depends on all remaining variables. Repeat this starting at i instead of k. There must be a (b, j) with $j \neq i$ such that $p[b, j]$ depends on all remaining variables. $\Box$

Corollary. If an algebra has a polynomial that depends on n-variables, $n > 0$, then it has a polynomial that depends on k variables for any k satisfying $1 \leq k \leq n$. $\Box$

For emphasis:

Corollary. Any minimal algebra $\mathbf{A}$ that is not essentially unary will have an essentially binary polynomial $q(x_1, x_2)$. Moreover, there will be elements $a, b \in A$ such that $q[a, 1] = q(a, y)$ and and $q[b, 2] = q(x, b)$ are permutations of A.

I will call such a binary polynomial a "q-polynomial", because when $\mathbf{A}$ is minimal and $|A| > 2$ we will see that q must be a quasigroup multiplication.

Minimal algebras with an essentially binary polynomial

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$.

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$.

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a;

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed.

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this <u>unary</u> function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the <u>binary</u> polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a,1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Theorem.

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a,1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Theorem. If $\mathbf{A}$ is a minimal algebra with more than two elements,

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a,1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Theorem. If $\mathbf{A}$ is a minimal algebra with more than two elements, and $q = q(x, y)$ is an essentially binary polynomial, then q is a quasigroup operation on A.

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Theorem. If $\mathbf{A}$ is a minimal algebra with more than two elements, and $q = q(x, y)$ is an essentially binary polynomial, then q is a quasigroup operation on A. ($q(a, x)$ and $q(x, a)$ are permutations for every a.)

Minimal algebras with an essentially binary polynomial

Let $q(x_1, x_2)$ be a binary polynomial of $\mathbf{A}$. Write $q_a(x_2)$ for $q[a, 1](x_2) = q(a, x_2)$. We may repeatedly compose this unary function of the variable x_2 with itself:

$$\begin{aligned} q_a(x_2) &= q(a, x_2) \\ q_a^2(x_2) &= q(a, q(a, x_2)) \\ q_a^3(x_2) &= q_a(q(a, q(a, x_2))) \end{aligned}$$

In fact, we don't have to specify the parameter a; let $q_{x_1}^k(x_2)$ be the binary polynomial obtained by iterating q in the second variable with the first variable fixed. We will use this notation when proving

Theorem. If $\mathbf{A}$ is a minimal algebra with more than two elements, and $q = q(x, y)$ is an essentially binary polynomial, then q is a quasigroup operation on A. ($q(a, x)$ and $q(x, a)$ are permutations for every a.)

Minimal algebras with an essentially binary polynomial

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary,

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables,

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact,

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x:

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$,

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e. The table for r:

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Minimal algebras with an essentially binary polynomial

If $q(x,y)$ is essentially binary, then there exists $a,b \in A$ such that $q(a,y)$ and $q(x,b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a,y)$ is a permutation while, for some b, $q(b,y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x,y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x,y)) = r(x,y)$, while $r(a,y) = y$ and $r(b,y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Choose $c \notin \{a,b\}$

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Choose $c \notin \{a, b\}$ and $d \in \{a, b\} \setminus \{e\}$.

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Choose $c \notin \{a, b\}$ and $d \in \{a, b\} \setminus \{e\}$. What is $r(c, d)$?

Minimal algebras with an essentially binary polynomial

If $q(x,y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a,y)$ and $q(x,b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a,y)$ is a permutation while, for some b, $q(b,y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x,y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x,y)) = r(x,y)$, while $r(a,y) = y$ and $r(b,y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Choose $c \notin \{a,b\}$ and $d \in \{a,b\} \setminus \{e\}$. What is $r(c,d)$? (There is no valid choice,

Minimal algebras with an essentially binary polynomial

If $q(x, y)$ is essentially binary, then there exists $a, b \in A$ such that $q(a, y)$ and $q(x, b)$ depend on their variables, hence are permutations. We would like to show that this statement is true in a way that is independent of the choices of a and b.

Assume that, for some a, $q(a, y)$ is a permutation while, for some b, $q(b, y)$ is constant. There must exist k such that $q_a^k(y) = y$. In fact, , there must exist some K such that $r(x, y) := q_x^K(y)$ is idempotent for any x: $r(x, r(x, y)) = r(x, y)$, while $r(a, y) = y$ and $r(b, y) = e$ for some e. The table for r:

r	a	b	c	d	e	$\cdots$
a	a	b	c	d	e	
b	e	e	e	e	e	
c				$?$	e	
d						
e						
$\vdots$						$\ddots$

Choose $c \notin \{a, b\}$ and $d \in \{a, b\} \setminus \{e\}$. What is $r(c, d)$? (There is no valid choice, so "$q(a, y)$ a permutation implies $q(b, y)$ a permutation" for all a, b.)

Now cite known results

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial.

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms:

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms:

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x,$$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \ \ (x/y)y = x,$$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y,$$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y, \;\; x(x\backslash y) = y.$$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y, \;\; x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y, \;\; x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y, \;\; x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.
3. Maltsev algebras support a commutator theory similar to the theory for groups.

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy\rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x\rangle$

$$(xy)/y = x, \;\; (x/y)y = x, \;\; x\backslash(xy) = y, \;\; x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.
3. Maltsev algebras support a commutator theory similar to the theory for groups.

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \quad (x/y)y = x, \quad x\backslash(xy) = y, \quad x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.
3. Maltsev algebras support a commutator theory similar to the theory for groups. In particular
    1. Nonabelianness can be witnessed by a binary polynomial $q(x, y)$ and elements $a, b, c, d \in A$ such that

$$q(a, c) = q(a, d) \quad \& \quad q(b, c) \neq q(b, d).$$

Now cite known results

We have that every essentially binary polynomial of a minimal algebra of size > 2 is a quasigroup polynomial. Now we cite results:

1. Every finite multiplication quasigroup $\langle A; xy \rangle$ has left and right division terms: $\langle A; xy, x/y, y\backslash x \rangle$

$$(xy)/y = x, \quad (x/y)y = x, \quad x\backslash(xy) = y, \quad x(x\backslash y) = y.$$

2. Every 'complete' quasigroup has a Maltsev term: $m(x, y, z) = (x/(y\backslash y))(y\backslash z)$.
3. Maltsev algebras support a commutator theory similar to the theory for groups. In particular
   1. Nonabelianness can be witnessed by a binary polynomial $q(x, y)$ and elements $a, b, c, d \in A$ such that

$$q(a, c) = q(a, d) \quad \& \quad q(b, c) \neq q(b, d).$$

   2. Abelian Maltsev algebras are polynomially equivalent to modules.

Summary

Summary

Employing commutator theory,

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module.

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1 y_1 + \cdots + b_k y_k + c.$$

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1 y_1 + \cdots + b_k y_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1y_1 + \cdots + b_ky_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1 y_1 + \cdots + b_k y_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

If $a \in R \setminus \{0, 1\}$, then this will be essentially binary, hence a quasigroup polynomial.

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1y_1 + \cdots + b_ky_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

If $a \in R \setminus \{0, 1\}$, then this will be essentially binary, hence a quasigroup polynomial. This forces a to be invertible in R.

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1 y_1 + \cdots + b_k y_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

If $a \in R \setminus \{0, 1\}$, then this will be essentially binary, hence a quasigroup polynomial. This forces a to be invertible in R. Hence R is a finite division ring.

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1y_1 + \cdots + b_ky_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

If $a \in R \setminus \{0, 1\}$, then this will be essentially binary, hence a quasigroup polynomial. This forces a to be invertible in R. Hence R is a finite division ring. A finite division ring is a field,

Summary

Employing commutator theory, we get that any minimal algebra of more than two elements that is not essentially unary must be polynomially equivalent to a module. That means that a typical polynomial operation of $\mathbf{A}$ will have the 'affine representation'

$$Q(x, \bar{y}) = ax + b_1 y_1 + \cdots + b_k y_k + c.$$

Every element of the associated ring occurs as the coefficient of x a binary polynomial operation with with affine representation

$$q(x, y) = ax + (1 - a)y.$$

If $a \in R \setminus \{0, 1\}$, then this will be essentially binary, hence a quasigroup polynomial. This forces a to be invertible in R. Hence R is a finite division ring. A finite division ring is a field, so $\mathbf{A}$ is polynomially equivalent to a vector space over a finite field.

Appendix

Appendix

I have been ignoring the 2-element case.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post –

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence'

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic).

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

Appendix

I have been ignoring the 2-element case. The clones on $\{0,1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0,1\};0,1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to ‘polynomial equivalence’ (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to ‘polynomial equivalence’ (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle \{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle \{0, 1\}; x', 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0,1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0,1\};0,1\rangle$. A G-set with $|G|=1$.
2. $\langle\{0,1\};x',0,1\rangle$. A G-set with $|G|=2$.
3. $\langle\{0,1\};+,0,1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle \{0, 1\}; 0, 1 \rangle$. A G-set with $|G| = 1$.
2. $\langle \{0, 1\}; x', 0, 1 \rangle$. A G-set with $|G| = 2$.
3. $\langle \{0, 1\}; +, 0, 1 \rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle \{0, 1\}; \wedge, 0, 1 \rangle$ or $\langle \{0, 1\}; \vee, 0, 1 \rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.
5. $\langle\{0, 1\}; \wedge, \vee, 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.
5. $\langle\{0, 1\}; \wedge, \vee, 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0,1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0,1\};0,1\rangle$. A G-set with $|G|=1$.
2. $\langle\{0,1\};x',0,1\rangle$. A G-set with $|G|=2$.
3. $\langle\{0,1\};+,0,1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0,1\};\wedge,0,1\rangle$ or $\langle\{0,1\};\vee,0,1\rangle$. A semilattice.
5. $\langle\{0,1\};\wedge,\vee,0,1\rangle$. A lattice.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.
5. $\langle\{0, 1\}; \wedge, \vee, 0, 1\rangle$. A lattice.
6. $\langle\{0, 1\}; \wedge, \vee, x', 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.
5. $\langle\{0, 1\}; \wedge, \vee, 0, 1\rangle$. A lattice.
6. $\langle\{0, 1\}; \wedge, \vee, x', 0, 1\rangle$.

Appendix

I have been ignoring the 2-element case. The clones on $\{0,1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0,1\};0,1\rangle$. A G-set with $|G|=1$.
2. $\langle\{0,1\};x',0,1\rangle$. A G-set with $|G|=2$.
3. $\langle\{0,1\};+,0,1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0,1\};\wedge,0,1\rangle$ or $\langle\{0,1\};\vee,0,1\rangle$. A semilattice.
5. $\langle\{0,1\};\wedge,\vee,0,1\rangle$. A lattice.
6. $\langle\{0,1\};\wedge,\vee,x',0,1\rangle$. A Boolean algebra.

Appendix

I have been ignoring the 2-element case. The clones on $\{0, 1\}$ were classified by Emil Post – there are countably many isomorphisms types. There are only six of them up to 'polynomial equivalence' (= the polynomial expansions of the associated algebras are weakly isomorphic). They are:

1. $\langle\{0, 1\}; 0, 1\rangle$. A G-set with $|G| = 1$.
2. $\langle\{0, 1\}; x', 0, 1\rangle$. A G-set with $|G| = 2$.
3. $\langle\{0, 1\}; +, 0, 1\rangle$. An $\mathbb{F}_2$-vector space.
4. $\langle\{0, 1\}; \wedge, 0, 1\rangle$ or $\langle\{0, 1\}; \vee, 0, 1\rangle$. A semilattice.
5. $\langle\{0, 1\}; \wedge, \vee, 0, 1\rangle$. A lattice.
6. $\langle\{0, 1\}; \wedge, \vee, x', 0, 1\rangle$. A Boolean algebra.