Monomial Clones

Hajime Machida

Tokyo, Japan

SSAOS 2016

Trojanovice, Czech Republic

September 3 4 5 6 7 8 9 2016

Joint work with J. Pantović (Novi Sad)

Outline

I Introduction

What is a clone?

For $k > 1$ let $\quad E_k = \{0, 1, \ldots, k-1\}$

$f(x_1, \ldots, x_n)$: n-variable *function* on E_k
i.e., $\quad f : (E_k)^n \longrightarrow E_k$

$\mathcal{O}_k^{(n)}$: the set of n-variable functions on E_k

$$\mathcal{O}_k = \bigcup_{n=1}^{\infty} \mathcal{O}_k^{(n)}$$

$e_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i$: (n-variable i-th) *projection*

$\mathcal{J}_k$: the set of *projections* on E_k

We define (functional) *"composition"* of functions in a usual way.

Example of composition

Given $f(x_1, x_2, x_3) \in \mathcal{O}_k^{(3)}$ and $g(x_1, x_2) \in \mathcal{O}_k^{(2)}$, an example of composition of f and g is

$$f(g(x_1, x_2), x_3, x_4).$$

Definition

$C \ (\subseteq \mathcal{O}_k)$: clone on E_k

$\iff$

(i) $C \supseteq \mathcal{J}_k$

(ii) C is closed under composition

Definition

$C \ (\subseteq \mathcal{O}_k)$: clone on E_k

$\Longleftrightarrow$

(i) $C \supseteq \mathcal{J}_k$

(ii) C is closed under composition

$\mathcal{L}_k$: the set of all clones on E_k,

" *lattice of clones* " on E_k

Definition

$C \ (\subseteq \mathcal{O}_k)$: clone on E_k

$\Longleftrightarrow$

(i) $C \supseteq \mathcal{J}_k$

(ii) C is closed under composition

$\mathcal{L}_k$: the set of all clones on E_k,

" *lattice of clones* " on E_k

$\mathcal{L}_k$ contains

- the greatest element: $\mathcal{O}_k$
- the least element: $\mathcal{J}_k$

Basic Facts on Clones

(1) For $k = 2$, $\mathcal{L}_2$: countable
completely known (E. Post)

(2) For $k \geq 3$, $\mathcal{L}_k$: continuum
mostly **un**known

Basic Facts on Clones

(1) For $k = 2$, $\mathcal{L}_2$: countable
completely known (E. Post)

(2) For $k \geq 3$, $\mathcal{L}_k$: continuum
mostly **un**known

(3) *Maximal clones*
For each $k \geq 2$, completely known (I. Rosenberg)

(4) *Minimal clones*
For $k = 2$, completely known (E. Post)
For $k = 3$, completely known (B. Csákány)
For $k = 4$, ???
For $k \geq 5$, very little is known

Introducing the structure of a field into E_k

We introduce the structure of a field into E_k.

For this purpose, it is required that

$$k = \text{a prime power},$$

i.e., $k = p^e$ for a prime p and a positive integer e.

Then, consider $E_k = \{0, 1, \ldots, k\}$ as the finite field $\mathrm{GF}(k)$.

Polynomials over K

For arbitrary field K and a positive integer n, an (n-variable) *polynomial* over K is an n-variable function

$$\sum_{0 \le i_1, \ldots, i_n \le e} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

for some $e \in \mathbb{N}$ and $a_{i_1, \ldots, i_n} \in K$.
In other words, a polynomial is a finite sum of terms.

Polynomials over K

For arbitrary field K and a positive integer n, an (n-variable) *polynomial* over K is an n-variable function

$$\sum_{0 \le i_1, \ldots, i_n \le e} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

for some $e \in \mathbb{N}$ and $a_{i_1,\ldots,i_n} \in K$.
In other words, a polynomial is a finite sum of terms.

Well-known: An n-variable function $f(x_1, \ldots, x_n)$ over K is uniquely expressed as a polynomial.

Quiz 1

Consider two functions f and g expressed as polynomials on $E_2\,(=\{0,1\})$.

1. $f(x,y) = x\,y + 1$
2. $g(x,y) = x\,y + x + y$

Quiz 1

Consider two functions f and g expressed as polynomials on $E_2\,(=\{0,1\})$.

1. $f(x,y) = x\,y + 1$
2. $g(x,y) = x\,y + x + y$

Q1 : Which function is stronger with respect to the 'productive power' by (functional) composition ?

Quiz 1 (EASY)

Consider two functions f and g expressed as polynomials on E_2 $(= \{0, 1\})$.

1. $f(x, y) = x\,y + 1$
2. $g(x, y) = x\,y + x + y$

Q1 : Which function is stronger with respect to the ‘productive power’ by (functional) composition ?

A : f is stronger.
In fact,

1. $f(x, y) = \mathrm{NAND}\,(x, y)$
2. $g(x, y) = \mathrm{OR}\,(x, y)$

Quiz 2

Consider three functions u, v and w expressed as polynomials on $E_3\,(=\{0,1,2\})$.

1. $u(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y$
2. $v(x,y) = x^2y^2 + xy^2 + x^2y + xy + x + y$
3. $w(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y + 1$

Quiz 2

Consider three functions u, v and w expressed as polynomials on $E_3\,(=\{0,1,2\})$.

1. $u(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y$
2. $v(x,y) = x^2y^2 + xy^2 + x^2y + xy + x + y$
3. $w(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y + 1$

Q2 : Which function is the weakest ?

Quiz 2 (HARD)

Consider three functions u, v and w expressed as polynomials on $E_3\,(=\{0,1,2\})$.

1. $u(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y$
2. $v(x,y) = x^2y^2 + xy^2 + x^2y + xy + x + y$
3. $w(x,y) = x^2y^2 + xy^2 + x^2y + 2xy + x + y + 1$

Q2 : Which function is the weakest ?

A : u is the weakest.

Quiz 2 (HARD)

Consider three functions u, v and w expressed as polynomials on $E_3 \, (= \{0, 1, 2\})$.

1. $u(x, y) = x^2 y^2 + x y^2 + x^2 y + 2xy + x + y$
2. $v(x, y) = x^2 y^2 + x y^2 + x^2 y + xy + x + y$
3. $w(x, y) = x^2 y^2 + x y^2 + x^2 y + 2xy + x + y + 1$

Q2 : Which function is the weakest ?

A : u is the weakest. In fact,

(1) $u(x, y)$ generates a minimal clone,

(2) $w(x, y)$ is Webb function ($= \max(x, y) + 1$) which is known to generate all functions on E_3, and

(3) $v(x, y)$ stays somewhere in-between.

How to get a polynomial corresponding to a function:

GIVEN: $f(x_1, \ldots, x_n)$

i.e., a mapping $f : K^n \longrightarrow K$

To GET: $$\sum_{0 \leq i_1, \ldots, i_n \leq e} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

How to get a polynomial corresponding to a function:

GIVEN: $f(x_1, \ldots, x_n)$

i.e., a mapping $f : K^n \longrightarrow K$

To GET: $$\sum_{0 \leq i_1, \ldots, i_n \leq e} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

METHOD: " Lagrange interpolation formula "

Example

Suppose $f(x, y, z)$ is a 3-variable function on $E_3 = \{0, 1, 2\}$.
For $a, b, c \in E_3$, define

$$t_{abc}(x, y, z) = \prod_{a' \in E_3 \setminus \{a\}} \frac{x - a'}{a - a'} \cdot \prod_{b' \in E_3 \setminus \{b\}} \frac{y - b'}{b - b'} \cdot \prod_{c' \in E_3 \setminus \{c\}} \frac{z - c'}{c - c'}$$

Then

$$t_{abc}(x, y, z) = \begin{cases} 1 & \text{if } x = a,\ y = b,\ z = c \\ 0 & \text{otherwise} \end{cases}$$

Hence

$$f(x, y, z) = \sum_{(a,b,c) \in E_3^3} f(a, b, c) \cdot t_{abc}(x, y, z)$$

In General

For an n-variable function $f(x_1, \ldots, x_n)$ on E_k, we have

$$f(x_1, \ldots, x_n) = \sum_{(a_1, \ldots, a_n) \in E_k^n} f(a_1, \ldots, a_n) \cdot t_{a_1 \ldots a_n}(x_1, \ldots, x_n)$$

where

$$t_{a_1 \ldots a_n}(x_1, \ldots, x_n) = \prod_{1 \leq i \leq n} \left(\prod_{a_i' \in E_k \setminus \{a_i\}} \frac{x_i - a_i'}{a_i - a_i'} \right)$$

Example Let $f(x, y, z)$ be a function defined by

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x$$

and

$$f(x, y, z) = 0 \qquad \text{if} \quad |\{x, y, z\}| = 3.$$

Example Let $f(x, y, z)$ be a function defined by

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x$$

and

$$f(x, y, z) = 0 \qquad \text{if} \quad |\{x, y, z\}| = 3.$$

Then

$$\begin{aligned} f(x, y, z) &= \frac{(x-1)(x-2)}{(0-1)(0-2)} \cdot \frac{y(y-2)}{1 \cdot (1-2)} \cdot \frac{z(z-2)}{1 \cdot (1-2)} + \cdots \\ &\quad + 2 \cdot \frac{(x-1)(x-2)}{(0-1)(0-2)} \cdot \frac{y(y-1)}{2 \cdot (2-1)} \cdot \frac{z(z-1)}{2 \cdot (2-1)} + \cdots \\ &\qquad \text{(sum of 12 products)} \\ &= 2x^2(y+z) + 2y^2(z+x) + 2z^2(x+y) \end{aligned}$$

$\square$

Monomials over K

An (n-variable) *monomial* over K is an n-variable polynomial consisting of one term, i.e.,

$$a\, x_1^{i_1} \cdots x_n^{i_n}$$

for $a \in K$ and $i_1, \ldots, i_n \in \mathbb{N}$.

Monomials over K

An (n-variable) *monomial* over K is an n-variable polynomial consisting of one term, i.e.,

$$a\, x_1^{i_1} \cdots x_n^{i_n}$$

for $a \in K$ and $i_1, \ldots, i_n \in \mathbb{N}$.

$\langle\langle$ In the rest of my talk, we shall take a more restrictive view of monomials. $\rangle\rangle$

Monomials over K

An (n-variable) *monomial* over K is an n-variable polynomial consisting of one term, i.e.,

$$a\, x_1^{i_1} \cdots x_n^{i_n}$$

for $a \in K$ and $i_1, \ldots, i_n \in \mathbb{N}$.

$\langle\langle$ In the rest of my talk, we shall take a more restrictive view of monomials. $\rangle\rangle$

An (n-variable) monomial m over K is a *monic monomial* if the coefficient of m is 1, i.e., if m is

$$x_1^{i_1} \cdots x_n^{i_n}$$

for $i_1, \ldots, i_n \in \mathbb{N}$.

In what follows, by a monomial we shall mean a monic monomial, that is,

$$\text{“ monomial } = x_1^{i_1} \cdots x_n^{i_n} \text{ ”}$$

In what follows, by a monomial we shall mean a monic monomial, that is,

$$\text{“ monomial } = x_1^{i_1} \cdots x_n^{i_n} \text{ ”}$$

A monomial clone is defined as follows.

In what follows, by a monomial we shall mean a monic monomial, that is,

$$\text{“ monomial } = x_1^{i_1} \cdots x_n^{i_n} \text{ ”}$$

A monomial clone is defined as follows.

Definition

A clone C over K is a *monomial clone* if C is generated by some monomial m over K, i.e., $C = \langle m \rangle$.

Finite Field

We review fundamental properties of finite fields.

Proposition

(1) For any prime power k, there exists a finite field K whose cardinality is k. It is unique up to isomorphism, and is denoted by $\mathrm{GF}(k)$.

(2) Over $\mathrm{GF}(k)$, it holds that $x^k = x$ for every $x \in \mathrm{GF}(k)$.

Hence, we have:

Corollary

Any n-variable monomial m over $\mathrm{GF}(k)$ is expressed as

$$m = x_1^{i_1} \cdots x_n^{i_n}$$

for some $i_1, \ldots, i_n$ with $0 < i_1, \ldots, i_n < k$.

II Monomial Clones on E_3

To determine all monomial clones on E_3

In this section we determine all monomial clones on E_3.

To determine all monomial clones on E_3

In this section we determine all monomial clones on E_3.

Before doing so, we describe monomial clones on E_2.

Monomial Clones on E_2

Considering the fact that $x^2 = x$ holds on E_2, it is immediate to see that there exist only two monomial clones over E_2.

They are:

(1) $\langle x_1 \rangle$

(2) $\langle x_1 x_2 \rangle$

Notice that

(1) $\langle x_1 \rangle$ is the least clone $\mathcal{J}_2$, and

(2) $\langle x_1 x_2 \rangle$ is the set of all monomials on E_2.

Monomial Clones on E_3

Now we study monomial clones on E_3.

Since the equality $x^3 = x$ holds on E_3, and $\mathrm{GF}(3)$ is commutative, monomials that need to be considered are

$$x_1 \cdots x_s \, x_{s+1}^2 \cdots x_{s+t}^2$$

for $s,\ t \geq 0$ and $s + t > 0$.

$s \backslash t$	0	1	2	3
0		$\boldsymbol{x}_1^2$	$\boldsymbol{x}_1^2\boldsymbol{x}_2^2$	$x_1^2x_2^2x_3^2$
1	$\boldsymbol{x}_1$	$\boldsymbol{x}_1\boldsymbol{x}_2^2$	$x_1x_2^2x_3^2$	$x_1x_2^2x_3^2x_4^2$
2	$\boldsymbol{x}_1\boldsymbol{x}_2$	$x_1x_2x_3^2$	$x_1x_2x_3^2x_4^2$	$x_1x_2x_3^2x_4^2x_5^2$
3	$\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$	$x_1x_2x_3x_4^2$	$x_1x_2x_3x_4^2x_5^2$	$x_1x_2x_3x_4^2x_5^2x_6^2$
4	$x_1x_2x_3x_4$	$x_1x_2x_3x_4x_5^2$	$x_1x_2x_3x_4x_5^2x_6^2$	$x_1x_2x_3x_4x_5^2x_6^2x_7^2$
5	$x_1x_2x_3x_4x_5$	$x_1x_2x_3x_4x_5x_6^2$	$x_1x_2x_3x_4x_5x_6^2x_7^2$	$x_1x_2x_3x_4x_5x_6^2x_7^2x_8^2$

Table : Monomials on E_3 (for small s and t)

$$x_1 \cdots x_s \, x_{s+1}^2 \cdots x_{s+t}^2 \qquad (s,\ t \geq 0,\ s+t > 0)$$

$\boxed{t = 0}$

Lemma

(i) $s \geq 2$: even $\Longrightarrow \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 \rangle$

(ii) $s \geq 3$: odd $\Longrightarrow \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 x_3 \rangle$

$\boxed{t = 0}$

Lemma

(i) $s \geq 2$: even $\implies \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 \rangle$

(ii) $s \geq 3$: odd $\implies \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 x_3 \rangle$

Claim 1 (M-clones generated by a monomial with $t = 0$)

(i) There are three monomial clones:

$$\langle x_1 \rangle, \ \langle x_1 \, x_2 \rangle \ \text{ and } \ \langle x_1 \, x_2 \, x_3 \rangle.$$

(ii) $\langle x_1 \rangle \;=\;$ the least clone $\mathcal{J}_3$
$\langle x_1 \, x_2 \rangle =$ the set of all monomials on E_3

(iii) $\langle x_1 \rangle \subset \langle x_1 \, x_2 \, x_3 \rangle \subset \langle x_1 \, x_2 \rangle$

(Note: $\subset$ denotes the strict inclusion)

$\boxed{t = 0}$

Lemma

(i) $s \geq 2$: even $\Longrightarrow \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 \rangle$

(ii) $s \geq 3$: odd $\Longrightarrow \langle x_1 \cdots x_s \rangle = \langle x_1 x_2 x_3 \rangle$

Claim 1 (M-clones generated by a monomial with $t = 0$)

(i) There are three monomial clones:

$$\langle x_1 \rangle, \ \langle x_1 \, x_2 \rangle \ \text{and} \ \langle x_1 \, x_2 \, x_3 \rangle.$$

(ii) $\langle x_1 \rangle$ = the least clone $\mathcal{J}_3$
$\langle x_1 \, x_2 \rangle$ = the set of all monomials on E_3

(iii) $\langle x_1 \rangle \subset \langle x_1 \, x_2 \, x_3 \rangle \subset \langle x_1 \, x_2 \rangle$

(Note: $\subset$ denotes the strict inclusion)

Proof (i) From Lemma. (ii) Trivial. (iii) The first inclusion is clear. For the second inclusion, see the next page. $\square$

Proof of "$\langle x_1\, x_2\, x_3 \rangle \subset \langle x_1\, x_2 \rangle$":

Let

$$\rho = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\}$$

Then

$$x_1 x_2 x_3 \in \operatorname{Pol} \rho \quad \text{but} \quad x_1 x_2 \notin \operatorname{Pol} \rho$$

Hence,

$$x_1\, x_2 \notin \langle x_1\, x_2\, x_3 \rangle$$

and

$$\langle x_1\, x_2\, x_3 \rangle \neq \langle x_1\, x_2 \rangle \qquad \square$$

$s \backslash t$	0	1	2	3
0		$\boldsymbol{x}_1^2$	$\boldsymbol{x}_1^2\boldsymbol{x}_2^2$	$x_1^2x_2^2x_3^2$
1	$\boldsymbol{x}_1$	$\boldsymbol{x}_1\boldsymbol{x}_2^2$	$x_1x_2^2x_3^2$	$x_1x_2^2x_3^2x_4^2$
2	$\boldsymbol{x}_1\boldsymbol{x}_2$	$x_1x_2x_3^2$	$x_1x_2x_3^2x_4^2$	$x_1x_2x_3^2x_4^2x_5^2$
3	$\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$	$x_1x_2x_3x_4^2$	$x_1x_2x_3x_4^2x_5^2$	$x_1x_2x_3x_4^2x_5^2x_6^2$
4	—	$x_1x_2x_3x_4x_5^2$	$x_1x_2x_3x_4x_5^2x_6^2$	$x_1x_2x_3x_4x_5^2x_6^2x_7^2$
5	—	$x_1x_2x_3x_4x_5x_6^2$	$x_1x_2x_3x_4x_5x_6^2x_7^2$	$x_1x_2x_3x_4x_5x_6^2x_7^2x_8^2$

Table : Monomials on E_3

$\boxed{t > 0}$

Lemma

For $t > 0$ we have:

(i) $s = 0 \implies \langle x_1^2 x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1^2 x_2^2 \rangle$

(ii) $s = 1 \implies \langle x_1 \; x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1 x_2^2 \rangle$

(iii) $s \geq 2$: even $\implies \langle x_1 \cdots x_s \; x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 \rangle$

(iv) $s \geq 3$: odd $\implies \langle x_1 \cdots x_s \; x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 x_3 \rangle$

Proof Easy from

$$x \cdot x^2 = x \quad \text{and} \quad x^2 \cdot x^2 = x^2. \qquad \square$$

$\boxed{t > 0}$

Lemma

For $t > 0$ we have:

(i) $s = 0 \implies \langle x_1^2 x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1^2 x_2^2 \rangle$

(ii) $s = 1 \implies \langle x_1 \, x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1 x_2^2 \rangle$

(iii) $s \geq 2$: even $\implies \langle x_1 \cdots x_s \, x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 \rangle$

(iv) $s \geq 3$: odd $\implies \langle x_1 \cdots x_s \, x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 x_3 \rangle$

Proof Easy from

$$x \cdot x^2 = x \quad \text{and} \quad x^2 \cdot x^2 = x^2.$$

□

Claim 2 (M-clones generated by a monomial with $t = 1$)

(i) There are two such clones $\langle x_1^2 \rangle$ and $\langle x_1 \, x_2^2 \rangle$.

(ii) $\langle x_1 \rangle \subset \langle x_1^2 \rangle \subset \langle x_1 \, x_2 \rangle$

(iii) $\langle x_1 \rangle \subset \langle x_1 \, x_2^2 \rangle \subset \langle x_1 \, x_2 \, x_3 \rangle$

$s \backslash t$	0	1	2	3
0		$\boldsymbol{x}_1^2$	$\boldsymbol{x}_1^2\boldsymbol{x}_2^2$	$x_1^2x_2^2x_3^2$
1	$\boldsymbol{x}_1$	$\boldsymbol{x}_1\boldsymbol{x}_2^2$	$x_1x_2^2x_3^2$	$x_1x_2^2x_3^2x_4^2$
2	$\boldsymbol{x}_1\boldsymbol{x}_2$	—	$x_1x_2x_3^2x_4^2$	$x_1x_2x_3^2x_4^2x_5^2$
3	$\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$	—	$x_1x_2x_3x_4^2x_5^2$	$x_1x_2x_3x_4^2x_5^2x_6^2$
4	—	—	$x_1x_2x_3x_4x_5^2x_6^2$	$x_1x_2x_3x_4x_5^2x_6^2x_7^2$
5	—	—	$x_1x_2x_3x_4x_5x_6^2x_7^2$	$x_1x_2x_3x_4x_5x_6^2x_7^2x_8^2$

Table : Monomials on E_3

$\boxed{t > 0}$

Lemma

For $t > 0$ we have:

(i) $s = 0 \implies \langle x_1^2 x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1^2 x_2^2 \rangle$

(ii) $s = 1 \implies \langle x_1\ x_2^2 \cdots x_{t+1}^2 \rangle = \langle x_1 x_2^2 \rangle$

(iii) $s \geq 2$: even $\implies \langle x_1 \cdots x_s\ x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 \rangle$

(iv) $s \geq 3$: odd $\implies \langle x_1 \cdots x_s\ x_{s+1}^2 \cdots x_{s+t}^2 \rangle = \langle x_1 x_2 x_3 \rangle$

Claim 3 (M-clones generated by a monomial with $t = 2$)

(i) There is only one such clone $\langle x_1^2\ x_2^2 \rangle$.

(ii) $\langle x_1^2 \rangle \subset \langle x_1^2\ x_2^2 \rangle \subset \langle x_1\ x_2 \rangle$

$s \backslash t$	0	1	2	3
0		$\boldsymbol{x}_1^2$	$\boldsymbol{x}_1^2\boldsymbol{x}_2^2$	—
1	$\boldsymbol{x}_1$	$\boldsymbol{x}_1\boldsymbol{x}_2^2$	—	—
2	$\boldsymbol{x}_1\boldsymbol{x}_2$	—	—	—
3	$\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$	—	—	—
4	—	—	—	—
5	—	—	—	—

Table : Monomials on E_3

Hence, monomial clones over E_3 are the following:

(1) $\langle x_1 \rangle$
(2) $\langle x_1\ x_2 \rangle$
(3) $\langle x_1\ x_2\ x_3 \rangle$
(4) $\langle x_1^2 \rangle$
(5) $\langle x_1\ x_2^2 \rangle$
(6) $\langle x_1^2\ x_2^2 \rangle$

For example, we show:

$\langle x_1^2\, x_2^2 \rangle$ and $\langle x_1\, x_2\, x_3 \rangle$ are incomparable.

Proof

(a) $\underline{\langle x_1^2\, x_2^2 \rangle \not\subset \langle x_1\, x_2\, x_3 \rangle}$

Let

$$\rho = \left\{ \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\}$$

Then

$$x_1 x_2 x_3 \in \mathrm{Pol}\,\rho \quad \text{but} \quad x_1^2 x_2^2 \notin \mathrm{Pol}\,\rho$$

Hence,

$$x_1^2\, x_2^2 \notin \langle x_1\, x_2\, x_3 \rangle$$

and

$$\langle x_1^2\, x_2^2 \rangle \not\subset \langle x_1\, x_2\, x_3 \rangle\,.$$

(b) $\underline{\langle x_1\, x_2\, x_3 \rangle \not\subset \langle x_1^2\, x_2^2 \rangle}$

Let

$$\tau = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}$$

Then

$$x_1^2 x_2^2 \in \operatorname{Pol} \tau \quad \text{but} \quad x_1 x_2 x_3 \notin \operatorname{Pol} \tau$$

Hence,

$$x_1\, x_2\, x_3 \notin \langle x_1^2 x_2^2 \rangle$$

and

$$\langle x_1\, x_2\, x_3 \rangle \not\subset \langle x_1^2\, x_2^2 \rangle\ .$$

From (a) and (b) we see that $\langle x_1^2\, x_2^2 \rangle$ and $\langle x_1\, x_2\, x_3 \rangle$ are incomparable. $\square$

Summary

(a1) $\langle x_1 \rangle \subset \langle x_1 x_2^2 \rangle \subset \langle x_1 x_2 x_3 \rangle \subset \langle x_1 x_2 \rangle$

(a2) $\langle x_1 \rangle \subset \langle x_1^2 \rangle \subset \langle x_1^2 x_2^2 \rangle \subset \langle x_1 x_2 \rangle$

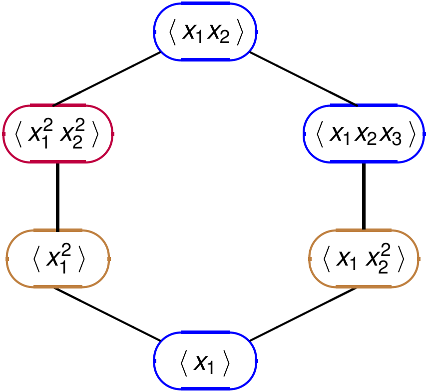
(b1) $\langle x_1^2 \rangle \not\subset \langle x_1 x_2^2 \rangle, \ \langle x_1 x_2^2 \rangle \not\subset \langle x_1^2 \rangle$

(b2) $\langle x_1^2 \rangle \not\subset \langle x_1 x_2 x_3 \rangle, \ \langle x_1 x_2 x_3 \rangle \not\subset \langle x_1^2 \rangle$

(b3) $\langle x_1^2 x_2^2 \rangle \not\subset \langle x_1 x_2^2 \rangle, \ \langle x_1 x_2^2 \rangle \not\subset \langle x_1^2 x_2^2 \rangle$

(b4) $\langle x_1^2 x_2^2 \rangle \not\subset \langle x_1 x_2 x_3 \rangle, \ \langle x_1 x_2 x_3 \rangle \not\subset \langle x_1^2 x_2^2 \rangle$

Case: $k = 3$



Note: $\langle x_1 x_2 \rangle$ $=$ the set of all monomials on E_3

$\langle x_1 \rangle = \mathcal{J}_3$

III Monomials $x^s y^t$

In this section we investigate monomial clones on E_k which are generated by unary functions (1-variable functions) and binary functions (2-variable functions).

We put emphasis on monomials which generate minimal clones in the lattice $\mathcal{L}_k$ of clones.

Let $\mathcal{M}_k$ be the set of monomial clones on E_k.

Remark

For any $C \in \mathcal{M}_k$,

$$C \text{ is minimal in } \mathcal{M}_k \implies C \text{ is minimal in } \mathcal{L}_k$$

(i.e., C is a minimal clone)

Let $\mathcal{M}_k$ be the set of monomial clones on E_k.

Remark

For any $C \in \mathcal{M}_k$,

$$C \text{ is minimal in } \mathcal{M}_k \quad \Longrightarrow \quad C \text{ is minimal in } \mathcal{L}_k$$

(i.e., C is a minimal clone)

Hence, we want to find:

monomial clones which are minimal in $\mathcal{M}_k$.

($=$ a motivation for the later study of 2-variable monomials)

Monomials x^s

As for unary functions generating minimal clones, the next fact is well-known.

Fact: A unary function $f \in \mathcal{O}_k^{(1)}$ generates a minimal clone if and only if

(1) f is a permutation of prime order, or

(2) f is not a permutation and satisfies $f \circ f = f$.

Now, when is a unary monomial x^s a permutation?

A (trivial) answer is:

Lemma

For a prime-power $k > 1$ and $0 < s < k$, the following are equivalent.

(1) x^s is a permutation on E_k

(2) $s^i \equiv 1 \pmod{k-1}$ for some $i > 1$

(3) s and $k-1$ are co-prime, i.e., $(s, k-1) = 1$.

(Remark: Due to Fermat-Euler Theorem)

Example: Unary minimal monomials for $k = 3, 5, 7, 11, 13$

(1) $k = 3$: $\langle x^2 \rangle$ is minimal.

(2) $k = 5$: $\langle x^s \rangle$ is minimal for $s = 3, 4$.
$$\langle x^4 \rangle \subset \langle x^2 \rangle$$

(3) $k = 7$: $\langle x^s \rangle$ is minimal for $s = 3, 4, 5, 6$.
$$\langle x^4 \rangle \subset \langle x^2 \rangle$$

(4) $k = 11$: $\langle x^s \rangle$ is minimal for $s = 5, 6, 9$.
$$\langle x^6 \rangle \subset \langle x^4 \rangle \subset \langle x^2 \rangle = \langle x^8 \rangle$$
$$\langle x^9 \rangle \subset \langle x^3 \rangle = \langle x^7 \rangle$$

(5) $k = 13$: $\langle x^s \rangle$ is minimal for $s = 4, 5, 6, 7, 9, 11$
$$\langle x^4 \rangle \subset \langle x^8 \rangle \subset \langle x^2 \rangle; \ \langle x^4 \rangle \subset \langle x^{10} \rangle$$
$$\langle x^9 \rangle \subset \langle x^3 \rangle$$

Monomials $x^s y^t$

Now, we consider 2-variable monomials $x^s y^t$ and clones generated by them. (For convenience we use x and y, instead of x_1 and x_2, for the variable symbols.)

More precisely, we consider

$$x^s y^t \qquad \text{for} \quad 0 < s,\, t < k$$

with the additional condition

$$s + t = k.$$

Note 1: If m is a monomial which generates a **non-unary minimal clone** then
(1) m must be a 2-variable monomial $x^s y^t$
and,
(2) since $\langle x^s y^t \rangle$ does not contain any non-trivial unary functions, the condition $s + t = k$ must be satisfied.

Note 1: If m is a monomial which generates a **non-unary minimal clone** then
(1) m must be a 2-variable monomial $x^s\, y^t$
and,
(2) since $\langle x^s\, y^t \rangle$ does not contain any non-trivial unary functions, the condition $s + t = k$ must be satisfied.

Note 2: For $u, v \in \mathbb{N}$ with $0 < u,\ v < k$,

$$x^u\, y^v \in \langle x^s\, y^t \rangle \quad \Longrightarrow \quad u + v = k$$

i.e., this condition on the exponents is *preserved* by composition.

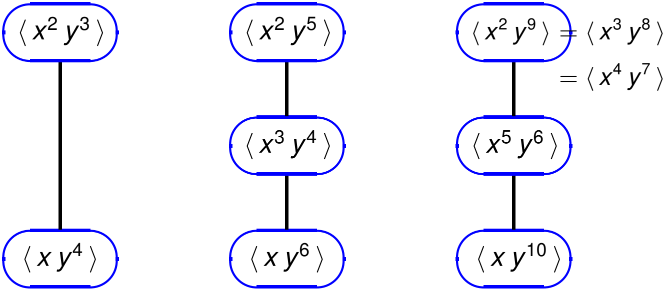
Note 1: If m is a monomial which generates a **non-unary minimal clone** then
(1) m must be a 2-variable monomial $x^s y^t$
and,
(2) since $\langle x^s y^t \rangle$ does not contain any non-trivial unary functions, the condition $\underline{s + t = k}$ must be satisfied.

Note 2: For $u, v \in \mathbb{N}$ with $0 < u, v < k$,

$$x^u y^v \in \langle x^s y^t \rangle \implies u + v = k$$

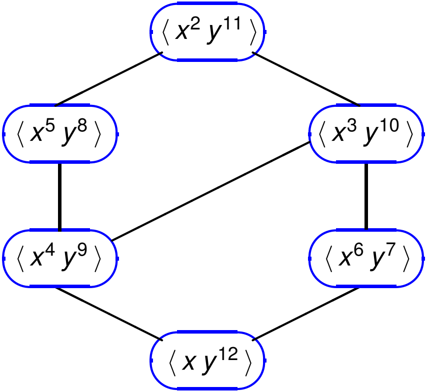
i.e., this condition on the exponents is *preserved* by composition.

Case: $k = 5, 7, 11$



$k = 5$ $\quad$ $k = 7$ $\quad$ $k = 11$

Case: $k = 13$


$\langle x^2 y^{11} \rangle$
$\langle x^5 y^8 \rangle$
$\langle x^3 y^{10} \rangle$
$\langle x^4 y^9 \rangle$
$\langle x^6 y^7 \rangle$
$\langle x y^{12} \rangle$

$$k = 13$$

Now, what observation do you get from these results ?

Now, what observation do you get from these results ?

My observation is:

One is weak, and two is strong !

Lemma

Let k be a prime power. For clones on $\mathrm{GF}(k)$ we have the following.

(1) $\langle x\, y^{k-1} \rangle \subseteq \langle x^2\, y^{k-2} \rangle$

(2) $\langle x^4\, y^{k-4} \rangle \subseteq \langle x^3\, y^{k-3} \rangle$

Lemma

Let k be a prime power. For clones on $\mathrm{GF}(k)$ we have the following.

(1) $\langle x\, y^{k-1} \rangle \subseteq \langle x^2\, y^{k-2} \rangle$

(2) $\langle x^4\, y^{k-4} \rangle \subseteq \langle x^3\, y^{k-3} \rangle$

Proof (i) Since

$$\begin{aligned}(k-2)^2 &= ((k-1)-1)^2 \\ &= (k-1)^2 - 2(k-1) + 1 \equiv 1 \pmod{k-1}\end{aligned}$$

we have $\quad x^2(x^2 y^{k-2})^{k-2} = x^{k-1} y.$

Lemma

Let k be a prime power. For clones on $\mathrm{GF}(k)$ we have the following.

(1) $\langle x\, y^{k-1} \rangle \subseteq \langle x^2\, y^{k-2} \rangle$

(2) $\langle x^4\, y^{k-4} \rangle \subseteq \langle x^3\, y^{k-3} \rangle$

Proof (i) Since

$$\begin{aligned} (k-2)^2 &= ((k-1)-1)^2 \\ &= (k-1)^2 - 2(k-1) + 1 \equiv 1 \pmod{k-1} \end{aligned}$$

we have $x^2(x^2y^{k-2})^{k-2} = x^{k-1}y$.

(ii) Similarly,

$$\begin{aligned} (k-3)^2 &= ((k-1)-2)^2 \\ &= (k-1)^2 - 4(k-1) + 4 \equiv 4 \pmod{k-1} \end{aligned}$$

implies $x^3(x^3y^{k-3})^{k-3} = x^{k-4}y^4$. $\square$

Two is strong

Proposition

For any prime power $k > 1$ and **any** $0 < s < k$, it holds

$$\langle x^s y^{k-s} \rangle \subseteq \langle x^2 y^{k-2} \rangle.$$

on $\mathrm{GF}(k)$.

Two is strong

Proposition

For any prime power $k > 1$ and **any** $0 < s < k$, it holds

$$\langle x^s y^{k-s} \rangle \subseteq \langle x^2 y^{k-2} \rangle.$$

on $\mathrm{GF}(k)$.

Proof Proof by induction.

Basis: $y^2(y^2x^{k-2})^{k-2} = x^{(k-2)^2} y^{2k-2} = xy^{k-1}$

Inductive Step:

$$(x^s y^{k-s})^2 x^{k-2} = x^{2s+k-2} y^{2k-2s} = x^{2s-1} y^{k-2s+1}$$
$$(x^s y^{k-s})^2 y^{k-2} = x^{2s} y^{3k-2s-2} = x^{2s} y^{k-2s}$$

$\square$

One is weak

Lemma

$\langle\, xy^{k-1} \,\rangle$ is minimal in $\mathcal{M}_k$.

Proof For any monomial m in $\langle\, xy^{k-1} \,\rangle \setminus \mathcal{J}_k$, it is easy to verify that $xy^{k-1} \in \langle\, m \,\rangle$. $\square$

Question: Is $\langle\, xy^{k-1}\,\rangle$ uniquely minimal in $\mathcal{M}_k$?

Question: Is $\langle xy^{k-1} \rangle$ uniquely minimal in $\mathcal{M}_k$?

Conjecture: YES,

Question: Is $\langle xy^{k-1} \rangle$ uniquely minimal in $\mathcal{M}_k$?

Conjecture: YES,

that is:

For any prime power $k > 1$ and any $0 < s < k$, it holds that

$$\langle xy^{k-1} \rangle \subseteq \langle x^s y^{k-s} \rangle,$$

in other words,

$$\underline{\underline{xy^{k-1} \in \langle x^s y^{k-s} \rangle}}.$$

Partial results concerning the conjecture

Lemma

Let $k = 2m + 1$. Then

$$xy^{k-1} \in \langle x^m y^{k-m} \rangle$$

Proof Note that $k - 1 = 2m$.

$$\begin{aligned}(x^m y^{m+1})^m (y^m x^{m+1})^{m+1} &= x^{m^2+(m+1)^2} y^{2m(m+1)} \\ &= xy^{2m} = xy^{k-1}\end{aligned}$$

$\square$

Lemma

For $k > 2$ and $1 < a < k$, if there exists $e > 1$ satisfying

$$\text{(i)} \quad a^e \equiv 1 \pmod{k-1}$$

or

$$\text{(ii)} \quad a^e \equiv a \pmod{k-1}$$

then $xy^{k-1} \in \langle x^a y^{k-a} \rangle$.

Lemma

For $k > 2$ and $1 < a < k$, if there exists $e > 1$ satisfying

$$\text{(i)} \quad a^e \equiv 1 \pmod{k-1}$$

or

$$\text{(ii)} \quad a^e \equiv a \pmod{k-1}$$

then $$xy^{k-1} \in \langle x^a y^{k-a} \rangle .$$

Proof (i) By repeating substitution of $x^a y^{k-a}$ into x e times, we obtain:

$$\begin{aligned} & ((\cdots((x^a y^{k-a})^a y^{k-a})^a \cdots)^a y^{k-a})^a y^{k-a} \\ = \; & x^{a^e} y^* \\ = \; & xy^{k-1} \end{aligned}$$

(ii) Similarly, we have:

$$\begin{aligned} & ((\cdots((x^a y^{k-a})^a y^{k-a})^a \cdots)^a y^{k-a})^a x^{k-a} \\ = \; & x^{a^e+(k-a)} y^* \\ = \; & x^{a+(k-a)} y^* \; = \; x^k y^{k-1} \; = \; xy^{k-1} \end{aligned}$$

$\square$

In most cases, the following property holds for $1 < a < k$.

$$(\exists\, e > 1)\ \ a^e \equiv a \pmod{k-1}$$

In most cases, the following property holds for $1 < a < k$.

$$(\exists\, e > 1) \;\; a^e \equiv a \pmod{k-1}$$

Example ($k = 11$) Table of $a^e \pmod{10}$

$a \setminus e$	1	2	3	4	5	$\cdots$
2	**2**	4	8	6	**2**	$\cdots$
9	**9**	1	**9**	$\cdots$		
3	**3**	9	7	1	**3**	$\cdots$
8	**8**	4	2	6	**8**	$\cdots$
4	**4**	6	**4**	$\cdots$		
7	**7**	9	3	1	**7**	$\cdots$
5	**5**	**5**	$\cdots$			
6	**6**	**6**	$\cdots$			

Counter-example ($k = 37$) Table of $a^e \pmod{36}$

$a \setminus e$	1	2	3	4	5	6	7	8
2	2	4	8	16	32	28	20	4
35	35	1	35		$\cdots$			
3	3	**9**	27	**9**		$\cdots$		
34	34	**4**	28	16	**4**	$\cdots$		
4	4	16	28	4		$\cdots$		
33	33	9	10	9		$\cdots$		

Counter-example ($k = 37$) Table of $a^e \pmod{36}$

$a \setminus e$	1	2	3	4	5	6	7	8
2	2	4	8	16	32	28	20	4
35	35	1	35		$\cdots$			
3	3	**9**	27	**9**		$\cdots$		
34	34	**4**	28	16	**4**	$\cdots$		
4	4	16	28	4		$\cdots$		
33	33	9	10	9		$\cdots$		

However, even in this case, $x\,y^{36} \in \langle x^3 y^{34} \rangle$ holds because

$$3^2 + 34^3 \equiv 9 + 28 \equiv 1 \pmod{36}$$

and

$$(x^3 y^{34})^3\,(y^3 (y^3 x^{34})^{34})^{34} = x\,y^{36}$$

Lemma

Let $k > 2$ be a prime and a be a positive integer. If a and $k-1$ are coprime, i.e., $\mathrm{GCD}(a, k-1) = 1$ then

$$xy^{k-1} \in \langle x^a y^{k-a} \rangle$$

Proof If there exists $e > 0$ such that $a^e \equiv 1 \pmod{k-1}$ then the result follows from (i) of the preceding Lemma. Otherwise, there exist d, e such that $1 < d < e$ satisfying $a^d \equiv a^e \pmod{k-1}$. Then we have

$$a^d(a^{e-d} - 1) \equiv 0 \pmod{k-1}.$$

Since $\mathrm{GCD}(a, k-1) = 1$, it follows that

$$a^{e-d} \equiv 1 \pmod{k-1},$$

which implies

$$x^{a^{e-d}} y^{k-a^{e-d}} = xy^{k-1}$$

and the conclusion follows. $\square$

One more property, which may be of interest:

Lemma

Let k be an odd prime power and suppose that

$$k = 2m + 1 \quad \left(\Leftrightarrow \; m = \frac{k-1}{2} \right)$$

for $m \geq 3$. Then, for every $s \in \{2, \ldots, m-1\}$, we have

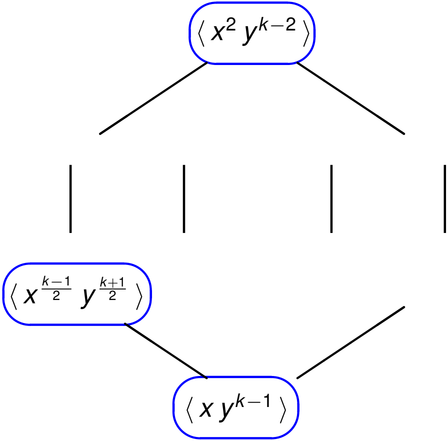
$$x^s y^{k-s} \notin \langle x^m y^{k-m} \rangle$$

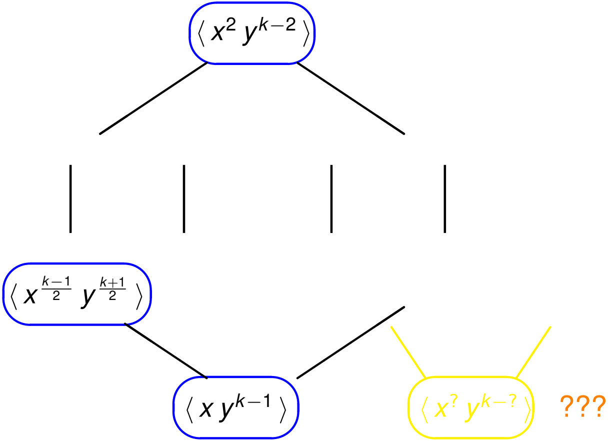
on $\mathrm{GF}(k)$.

Proof Note that $k-1=2m$. We can show below that all of m^2, $(m+1)^2$ and $m(m+1)$ are equivalent to one of 0, 1, m and $m+1$ mod $k-1$. Here the equivalence ($\equiv$) is taken for mod $k-1$.

$$
\begin{aligned}
m^2 &= \begin{cases} m(m-1)+m \equiv m & \text{if } m : \text{odd} \\ m \cdot m \equiv 0 & \text{if } m : \text{even} \end{cases} \\
(m+1)^2 &= m^2+2m+1 \equiv m^2+1 \\
&\equiv \begin{cases} m+1 & \text{if } m : \text{odd} \\ 1 & \text{if } m : \text{even} \end{cases} \\
m(m+1) &\equiv \begin{cases} 0 & \text{if } m : \text{odd} \\ m^2+m = m & \text{if } m : \text{even} \end{cases}
\end{aligned}
$$

Hence, among $x^s y^{k-s}$ for $s \in \{1,\ldots,m\}$, the terms that can be produced from $x^m y^{k-m}$ by composition are only xy^{k-1} and $x^m y^{k-m}$. $\square$


$\langle x^2 y^{k-2} \rangle$
$\langle x^{\frac{k-1}{2}} y^{\frac{k+1}{2}} \rangle$
$\langle x y^{k-1} \rangle$


$\langle x^2 y^{k-2} \rangle$
$\langle x^{\frac{k-1}{2}} y^{\frac{k+1}{2}} \rangle$
$\langle x y^{k-1} \rangle$
$\langle x^? y^{k-?} \rangle$
???

Thank you

for your attention !