Congruence Preservation and Recognizability

I. Guessarian
IRIF, CNRS & Université Denis Diderot-Paris 7

Joint work with

Patrick Cégielski & Serge Grigorieff

(Université Paris 12) (Université Paris 7)

31/01/2019

Outline

1. Original problem
2. Characterize Congruence Preservation Algebraically
3. Characterize Congruence Preservation via Lattice Closure
4. More on Algebras, Congruence preservation, Lattice closure
5. Case of $\mathbb{Z}$

Outline

1 Original problem

2 Characterize Congruence Preservation Algebraically

3 Characterize Congruence Preservation via Lattice Closure

4 More on Algebras, Congruence preservation, Lattice closure

5 Case of $\mathbb{Z}$

A Question by Jean-Eric Pin

$\mathcal{L}$ lattice of finite subsets of $\mathbb{N}$, (i.e. for $L, L' \in \mathcal{L}$, $L \cap L',\ L \cup L' \in \mathcal{L}$)

$\mathcal{L}$ closed under decrement $\overset{?}{\Longrightarrow}$ $\mathcal{L}$ closed under division

Closure under decrement: $\forall L \in \mathcal{L}$:
$(L-1) = \{n-1 \mid n \in L, n-1 \geq 0\} \in \mathcal{L}$ $\qquad \{0,3,7\} - 1 = \{2,6\}$

Closure under division: $\forall a \in \mathbb{N}, \forall L \in \mathcal{L}$:
$L/a = \{n \mid an \in L\} \in \mathcal{L}$ $\qquad \{0,3,7\}/3 = \{0,1\}$

Answer : YES ... and Much More. . .

Which functions $f:\mathbb{N}\to\mathbb{N}$ are such that

$$\forall\mathcal{L} \text{ lattice of finite subsets of } \mathbb{N}$$
$$\forall L\in\mathcal{L}\ \ (L-1)\in\mathcal{L} \implies \forall L\in\mathcal{L}\ \ f^{-1}(L)\in\mathcal{L} \qquad (*)$$

Theorem (CGG13)

$f:\mathbb{N}\to\mathbb{N}$ satisfies (*) $\iff$ f is congruence preserving

Idem for lattices of regular subsets of $\mathbb{N}$

[CGG13] *On Lattices of Regular Sets of Natural Integers Closed under Decrementation*, IPL (2013).

Definition

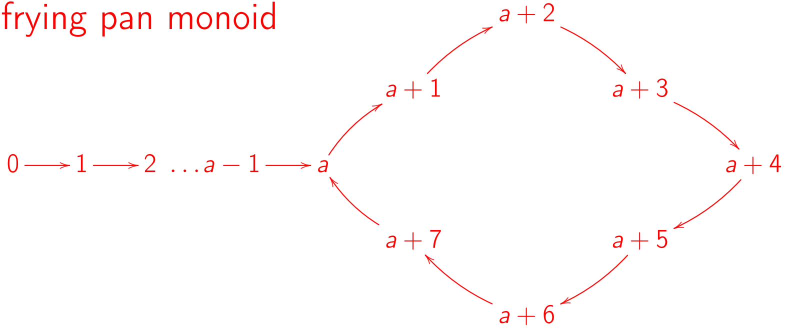
f congruence preserving $\iff$
for any congruence $\sim$ on $\mathbb{N}$: $x\sim y \implies f(x)\sim f(y)$

Congruences on $\langle \mathbb{N}, + \rangle$

$x \sim y$ iff; either $x = y$ or $\varphi(x) = \varphi(y)$ with φ

$$\varphi(x) = \begin{cases} x & \text{for } x \leq a \\ a + (\ (x-a) \mod k\ ) & \text{for } x > a \end{cases} \qquad a \geq 0, k \geq 1$$

frying pan monoid



$a \sim a+8 \sim a+16 \sim \cdots$ or $a+3 \sim a+11 \sim a+19 \sim \cdots$

Morphisms, Congruences depend on signature

- Morphism on $\langle \mathbb{N}, + \rangle \not\Leftrightarrow$ Morphism on $\langle \mathbb{N}, \times \rangle$

  $\varphi(x) = 3x$ $\quad\quad$ $\psi(x) = \begin{cases} 1 \text{ iff } \exists n \; x = 2^n, \\ 0 \text{ otherwise.} \end{cases}$

- $\langle \mathbb{N}, + \rangle$-congruence $\Longrightarrow$ $\langle \mathbb{N}, \times \rangle$-congruence.
  $\langle \mathbb{N}, + \rangle$ -congruence $\not\Leftarrow$ $\langle \mathbb{N}, \times \rangle$-congruence.

  $x \sim y$ iff $\psi(x) = \psi(y)$ is a $\langle \mathbb{N}, \times \rangle$-congruence and not a $\langle \mathbb{N}, + \rangle$ -congruence: $2 \sim 4$ and $4 \sim 4$ but $(2 + 4) \not\sim (4 + 4)$

Issue: capture congruence preservation

Theorem (CGG13)

$f : \mathbb{N} \to \mathbb{N}$ *congruence preserving* $\iff$

1. $\forall a, b \in \mathbb{N} \quad a - b$ *divides* $f(a) - f(b)$ *or*
   equivalently (justifying the denomination), $\forall n \geq 1$,
   $$\forall a, b \in \mathbb{N} \;\; (\; a \equiv b \bmod n \implies f(a) \equiv f(b) \bmod n \;)$$
2. *and* $\forall a \in \mathbb{N} \quad f(a) \geq a$ *or f constant*

- Obvious example: Polynomials in $\mathbb{N}[x]$
- What else ?

Congruence preserving functions

$\mathcal{A} = \langle A, \mathcal{O} \rangle$ algebra with operations $\mathcal{O}$.

Definition

$f : A^n \to A$ is congruence preserving iff, for any $\mathcal{O}$-congruence $\sim$ on A:

$\forall x_1, \ldots, x_n, y_1, \ldots, y_n \in A$

$$\bigwedge_{i=1}^{i=n} x_i \sim y_i \quad \Longrightarrow \quad f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n)$$

Example: "Polynomial functions" = expressed by terms with constants in A. What else ?

Outline

1 Original problem

2 Characterize Congruence Preservation Algebraically

3 Characterize Congruence Preservation via Lattice Closure

4 More on Algebras, Congruence preservation, Lattice closure

5 Case of $\mathbb{Z}$

Representing functions $\mathbb{N} \to \mathbb{Z}$

We represent functions $\mathbb{N} \to \mathbb{Z}$ by
series of polynomials in $\mathbb{Q}[x]$ mapping $\mathbb{N}$ into $\mathbb{Z}$

Binomial polynomial function $\mathbb{N} \to \mathbb{N}$ in $\mathbb{Q}[x]$

$$\binom{x}{0} = 1 \qquad \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

Representing functions $\mathbb{N} \to \mathbb{Z}$

Functions $\mathbb{N} \to \mathbb{Z}$ $\overset{1\text{-}1}{\equiv}$
Infinite $\mathbb{Z}$-linear combinations of the binomial polynomials

NO CONVERGENCE PROBLEM: For every $x \in \mathbb{N}$
infinite sum $\sum_{n\in\mathbb{N}} a_n \binom{x}{n}$ reduces to the finite sum $\sum_{n\leq x} a_n$

Characterize preservation of modular congruences

Theorem (CGG15)

If $f : \mathbb{N} \longrightarrow \mathbb{Z}$, *then* *(1)* $\Longleftrightarrow$ *(2)*

(1) $\forall x, y$ $\boxed{x - y \textit{ divides } f(x) - f(y)}$

(2) $f(x) = a_0 + a_1 x + a_2 \dfrac{x(x-1)}{2!} + a_3 \dfrac{x(x-1)(x-2)}{3!} + \cdots,$

where ℓ *divides* a_n *for all* $2 \leq \ell \leq n$.

[CGG15] *Newton representation of functions over natural integers having integral difference ratios*, Int. Jour. of Number Theory, (2015).

Characterize congruence preservation on $\mathbb{N}$

$f : \mathbb{N} \to \mathbb{N}$ congruence preserving $\iff$

1. $\forall a, b \in \mathbb{N} \quad a - b$ divides $f(a) - f(b)$
2. and $\forall x \in \mathbb{N} \quad f(x) \geq x$ or f constant.

Theorem

$f : \mathbb{N} \longrightarrow \mathbb{N}$ *Congruence preserving* $\iff$ *(1) and (2)*

(1) $f(x) = a_0 + a_1 x + a_2 \frac{x(x-1)}{2!} + a_3 \frac{x(x-1)(x-2)}{3!} + \cdots,$
where ℓ *divides* a_n *for all* $2 \leq \ell \leq n$

(2) $\forall x \in \mathbb{N} \quad f(x) \geq x$ *or* f *constant.*

Characterize congruence preservation on $\mathbb{N}$

$f : \mathbb{N} \to \mathbb{N}$ congruence preserving $\iff$

1. $\forall a, b \in \mathbb{N} \quad a - b$ divides $f(a) - f(b)$
2. and $\forall x \in \mathbb{N} \quad f(x) \geq x$ or f constant.

Theorem

$f : \mathbb{N} \longrightarrow \mathbb{N}$ *Congruence preserving* $\iff$ *(1) and (2)*

(1) $f(x) = a_0 + a_1 x + a_2 \dfrac{x(x-1)}{2!} + a_3 \dfrac{x(x-1)(x-2)}{3!} + \cdots,$ *where ℓ divides a_n for all $2 \leq \ell \leq n$*

(2) $\forall x \in \mathbb{N} \quad f(x) \geq x$ *or* f *constant.*

Corollary (CGG)

Non polynomial congruence preserving functions $\mathbb{N} \to \mathbb{N}$

$$f(x) = \lfloor e^{1/a} a^x x! \rfloor \quad \textit{for } a \in \mathbb{N} \setminus \{0, 1\}$$

third kind Bessel function g

$$g(x) \ = \frac{\Gamma(1/2)}{2 \times 4^x \times x!} \int_1^\infty e^{-t/2} (t^2 - 1)^x dt$$

Idem for $f(x) = \lceil e^{1/a} a^x x! \rceil$

[CGG] *Integral Difference Ratio Functions on Integers*, LNCS 8808 (2014).

- What about other algebras ??

Agebraic characterization of congruence preservation

Abbrev: CP= congruence preserving

f CP on $\langle \mathbb{N}, + \rangle \iff f$ infinite $\mathbb{Z}$-linear combination of binomial polynomials satisfying some conditions

- On $\mathbb{Z}, \mathbb{Z}_p$ with $+$ and $\times$: similar to $\mathbb{N}$
- On $\langle \mathbb{N}, \times \rangle$: much simpler characterization

Theorem

$f : \mathbb{N} \longrightarrow \mathbb{N}$;

$$f \text{ CP on } \langle \mathbb{N}, \times \rangle$$
$$\Updownarrow$$
$$f(x) = f(1) \times x^k, \text{ with } k \in \mathbb{N}$$

Agebraic characterization of congruence preservation

Abbrev: CP= congruence preserving

f CP on $\langle \mathbb{N}, + \rangle \iff f$ infinite $\mathbb{Z}$-linear combination of binomial polynomials satisfying some conditions

- On $\mathbb{Z}, \mathbb{Z}_p$ with $+$ and $\times$: similar to $\mathbb{N}$
- On $\langle \mathbb{N}, \times \rangle$: much simpler characterization

Theorem

$f : \mathbb{N} \longrightarrow \mathbb{N}$;

$$f \text{ CP on } \langle \mathbb{N}, \times \rangle$$

$$\Updownarrow$$

$$f(x) = f(1) \times x^k, \text{ with } k \in \mathbb{N}$$

Agebraic characterization of congruence preservation

Abbrev: CP= congruence preserving

f CP on $\langle \mathbb{N}, + \rangle \iff f$ infinite $\mathbb{Z}$-linear combination of binomial polynomials satisfying some conditions

- On $\mathbb{Z}, \mathbb{Z}_p$ with $+$ and $\times$: similar to $\mathbb{N}$
- On $\langle \mathbb{N}, \times \rangle$: much simpler characterization

Theorem

$f : \mathbb{N} \longrightarrow \mathbb{N}$;

$$f \text{ } CP \text{ on } \langle \mathbb{N}, \times \rangle$$
$$\Updownarrow$$
$$f(x) = f(1) \times x^k, \text{ with } k \in \mathbb{N}$$

Congruence preservation on a non commutative algebras

f CP on $\langle \mathbb{N}, \times \rangle \iff f(x) = f(1) \times x^k,\ k \in \mathbb{N}$.

Theorem

On the algebra of words with concatenation, $\mathcal{S} = \langle \Sigma^*, \cdot \rangle$
f CP $\iff f : x \mapsto w_0 x w_1 x w_2 \cdots x w_k$,
$k \in \mathbb{N},\ w_0, w_1, \ldots, w_k \in \Sigma^*$.

Non trivial proof using restricted morphisms.

affine complete algebras: for all f, f CP $\iff$ f polynomial.

- $\mathcal{S}$, $\langle \mathbb{N}, \times \rangle$ are affine complete.
- $\langle \mathbb{N}, + \rangle$ is not affine complete

Outline

1 Original problem

2 Characterize Congruence Preservation Algebraically

3 Characterize Congruence Preservation via Lattice Closure

4 More on Algebras, Congruence preservation, Lattice closure

5 Case of $\mathbb{Z}$

Congruence Preservation vs Closure of Lattices of Recognizable Sets

Theorem (CGG14)

Algebra $\mathcal{N} = \langle \mathbb{N}, + \rangle$, $f : \mathbb{N} \longrightarrow \mathbb{N}$, *then* (1) $\Longleftrightarrow$ (2)

(1) f *CP on* $\mathcal{N}$ *and*, $\forall a \in \mathbb{N}$, $f(a) \geq a$,

(2) *for every recognizable subset* L *of* $\mathcal{N}$ *the smallest lattice of subsets of* $\mathbb{N}$ *containing* L *and closed under* $x \mapsto x - 1$ *is also closed under* f^{-1}.

[CGG14] *On lattices of regular sets of natural integers closed under decrementation*, IPL 114 (2014).

- What about other algebras ??

Is congruence preservation characterized via lattice closure for any algebra?

Theorem ((1) $\Longleftrightarrow$ (2) on $\mathcal{N} = \langle \mathbb{N}, + \rangle$)

(1) f CP on $\mathcal{N}$ and, $\forall a \in \mathbb{N}$, $f(a) \geq a$,
(2) for every recognizable subset L of $\mathcal{N}$ the smallest lattice of subsets of $\mathbb{N}$ containing L and closed under $x \mapsto x - 1$ is also closed under f^{-1}.

Can be generalized to arbitrary algebras?

Theorem ((1) $\Longleftrightarrow$ (2) on $\mathcal{A} = \langle A, \mathcal{O} \rangle$)

(1) f CP on $\mathcal{A}$ and, something else,
(2) for every recognizable subset L of $\mathcal{A}$ the smallest lattice $\mathcal{L}_{\mathcal{A}}(L)$ of subsets of A containing L and closed under some operations is also closed under f^{-1}.

Recognizability in algebra $\mathcal{A} = \langle A, \mathcal{O} \rangle$

Definition

L is recognizable iff $L = \varphi^{-1}(F)$ with $\varphi \colon A \to M$ morphism, M a finite algebra with same signature as $\mathcal{A}$, $F \subset M$.

Examples

- $\langle \mathbb{N}, + \rangle$-recognizable: finite sets , $1 + 3\mathbb{N}$,
  $\{2\} \cup \{\ \{5, 7\} + 8\mathbb{N}\ \}$,
  $F \cup \{F' + k\mathbb{N}\}$ (general form)
- $\langle \mathbb{Z}, + \rangle$-recognizable: $F + k\mathbb{Z}$ (general form)
- $\langle \Sigma^*, \cdot \rangle$-recognizable: regular sets.

Recognizability depends on signature

$\langle \mathbb{N}, + \rangle$-recognizable $\Longrightarrow$ $\langle \mathbb{N}, \times \rangle$-recognizable.
$\langle \mathbb{N}, + \rangle$-recognizable $\not\Longleftarrow$ $\langle \mathbb{N}, \times \rangle$-recognizable.

$(1 + 3\mathbb{N})$ is $\langle \mathbb{N}, +, \times \rangle$-recognizable, but $\{2^n \mid n \in \mathbb{N}\}$ is $\langle \mathbb{N}, \times \rangle$-recognizable and not $\langle \mathbb{N}, + \rangle$-recognizable.

- $\langle \mathbb{N}, \times \rangle$-recognizables:
  1. all $\langle \mathbb{N}, + \rangle$-recognizables $(L = F \cup \{F' + k\mathbb{N}\})$,
  2. all finite unions $p_1^{L_1} \cdots p_n^{L_n}$, with $p_1, \ldots, p_n$ primes in P, $L_1, \ldots, L_n$ $\langle \mathbb{N}, + \rangle$-recognizable.
  3. suitably completed

Generalization to algebra: $\mathcal{N}_\times = \langle \mathbb{N}, \times \rangle$

Theorem ((1) $\Longleftrightarrow$ (2) on $\mathcal{N}_\times = \langle \mathbb{N}, \times \rangle$)

(1) f CP on $\mathcal{N}_\times$ and, $\forall a \in \mathbb{N}$, a divides $f(a)$,
(2) for every recognizable subset L of $\mathcal{N}_\times$ the smallest lattice $\mathcal{L}_{\mathcal{N}_\times}(L)$ of subsets of $\mathbb{N}$ containing L and closed under division is also closed under f^{-1}.

Division: $S \subset \mathbb{N}$, $a \in \mathbb{N}$, let $S/a = \{x/a \mid x \in S \text{ and } x/a \in \mathbb{N}\}$

$$(9 + 5\mathbb{N})/5 = \emptyset$$

$$\begin{aligned}(9 + 5\mathbb{N})/4 &= \{9, 14, 19, 24, 29, 34, 39, 44, \dots\}/4 \\ &= \{6, 11, 16 \dots\} = 6 + 5\mathbb{N}\end{aligned}$$

Tentative Generalization to Algebra $\mathcal{A} = \langle A, \mathcal{O} \rangle$

$gen(a, A, \mathcal{O})$ = set generated by a in $\mathcal{A}$.
– $gen(a, \mathbb{N}, +) = \{a + n \mid n \in \mathbb{N}\}$
– $gen(a, \mathbb{N}, \times) = \{a \times n \mid n \in \mathbb{N}\}$
– words with concatenation :
$gen(a, \Sigma^*, \cdot) = \{w \cdot a \cdot w' \mid w, w' \in \Sigma^*\}$

Theorem ((1) $\Longleftrightarrow$ (2) ???)

(1) f CP on $\mathcal{A}$ and, $\forall a \in A,\ f(a) \in gen(a, A, \mathcal{O})$
(2) for every recognizable subset L of $\mathcal{A}$ the smallest lattice $\mathcal{L}_{\mathcal{A}}(L)$ of subsets of A containing L and closed under o^{-1} for all $o \in \mathcal{O}$ is also closed under f^{-1}.

Affine complete algebras

Theorem

In algebra $\mathcal{A} = \langle A, \mathcal{O} \rangle$, if $f : A \to A$ defined by a polynomial and L recognizable, then $f^{-1}(L)$ recognizable.

Algebra $\mathcal{A} = \langle A, \mathcal{O} \rangle$ is affine complete if:

for all f, f CP $\iff$ f polynomial.

PROBLEM: $f^{-1}(L)$ in lattice??

WHAT ELSE??

Outline

1. Original problem
2. Characterize Congruence Preservation Algebraically
3. Characterize Congruence Preservation via Lattice Closure
4. More on Algebras, Congruence preservation, Lattice closure
5. Case of $\mathbb{Z}$

To which structures does the lattice closure characterization of CP extend ?

- Goal: generalize the algebraic characterization of congruence preservation via lattices to algebras beyond $\mathbb{N}$
- stable preorder preservation characterized via closure of lattices.
- congruence preservation characterized via closure of boolean algebras.
- except in some cases ....

Stable Preorder vs Congruence Preservation on $\mathcal{A} = \langle A, \mathcal{O} \rangle$

Theorem

(1) f *SPP on* $\mathcal{A}$ *and,* $\forall a \in A$, $f(a) \in gen(a, A, \mathcal{O})$
(2) for every subset L *of* $\mathcal{A}$ *the smallest complete lattice* $\mathcal{L}^{\infty}_{\mathcal{A}}(L)$ *of subsets of* A *containing* L *and closed under* o^{-1} *for all* $o \in \mathcal{O}$ *is also closed under* f^{-1}.

Theorem

(1) f *CP on* $\mathcal{A}$ *and,* $\forall a \in A$, $f(a) \in gen(a, A, \mathcal{O})$
(2) for every subset L *of* $\mathcal{A}$ *the smallest complete boolean algebra* $\mathcal{B}^{\infty}_{\mathcal{A}}(L)$ *of subsets of* A *containing* L *and closed under* o^{-1} *for all* $o \in \mathcal{O}$ *is also closed under* f^{-1}.

Sufficient conditions to characterize Congruence Preservation via Lattice closure

If $f : A \to A$, and $\mathcal{A} = \langle A, \mathcal{O} \rangle$

– residually finite algebra

– containing a group operation,

then congruence preservation is characterized via lattices

f CP and $\forall a \in A$, $f(a) \in gen(a, A, \mathcal{O})$

$$\Updownarrow$$

for every recognizable L, the smallest lattice $\mathcal{L}_{\mathcal{A}}(L)$ of subsets of A containing L and closed under o^{-1} for all $o \in \mathcal{O}$ is also closed under f^{-1}.

Outline

1 Original problem

2 Characterize Congruence Preservation Algebraically

3 Characterize Congruence Preservation via Lattice Closure

4 More on Algebras, Congruence preservation, Lattice closure

5 Case of $\mathbb{Z}$

$\mathcal{Z} = \langle \mathbb{Z}, + \rangle$

Theorem

$\mathcal{Z} = \langle \mathbb{Z}, + \rangle$, $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. 1 $\iff$ 2 $\iff$ 3 $\iff$ 4

1. f is CP on $\mathcal{Z}$.
2. $|x - y|$ divides $|f(x) - f(y)|$ for all $x, y \in \mathbb{Z}$.
3. For every recognizable subset L of $\mathcal{Z}$, the lattice $\mathcal{L}_{\mathcal{Z}}(L)$ is closed under f^{-1}.
4. $f(x) = \sum_{n \in \mathbb{N}} a_n P_n(x)$ where, for all $2 \leq \ell \leq n$, ℓ divides a_n.

Similar theorem for $\mathcal{Z} = \langle \mathbb{Z}, +, \times \rangle$ and $\mathcal{Z}_p = \langle \mathbb{Z}_p, +, \times \rangle$

Conclusion

- moral of the story: CP functions correspond to functions definable in terms of the algebra operations... in general ...
- affine complete non commutative algebras different from the free monoid ?

THANKS FOR YOUR ATTENTION