Generalisation of Canonical Number Systems

Paul Surer (joint work with K. Scheicher, J. M. Thuswaldner and C. Van de Woestijne)

Montanuniversität Leoben
Department of Mathematics and Information Technology
Chair of Mathematics and Statistics
8700 Leoben - AUSTRIA

Prague, May 2008

Supported by FWF, project S9610

Canonical Number Systems

Definition (Pethő, 1991)

Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0$, $|p_0| \geq 2$, $\mathcal{R} = \mathbb{Z}[x]/(P)$, X the image of x under the canonical epimorphism and $\mathcal{N} = [0, |p_0|) \cap \mathbb{Z}$. $(P, \mathcal{N})$ is called a Canonical Number System (CNS) if each $A \in \mathcal{R}$ can be represented as

$$A = \sum_{j=0}^{k} a_j X^j, \quad a_j \in \mathcal{N}.$$

Canonical Number Systems

Definition (Pethő, 1991)

Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0$, $|p_0| \geq 2$, $\mathcal{R} = \mathbb{Z}[x]/(P)$, X the image of x under the canonical epimorphism and $\mathcal{N} = [0, |p_0|) \cap \mathbb{Z}$. $(P, \mathcal{N})$ is called a Canonical Number System (CNS) if each $A \in \mathcal{R}$ can be represented as

$$A = \sum_{j=0}^{k} a_j X^j, \quad a_j \in \mathcal{N}.$$

Examples of generalisations

- Akiyama *et al.*, $\frac{3}{2}$-problem,

Canonical Number Systems

Definition (Pethő, 1991)

Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0$, $|p_0| \geq 2$, $\mathcal{R} = \mathbb{Z}[x]/(P)$, X the image of x under the canonical epimorphism and $\mathcal{N} = [0, |p_0|) \cap \mathbb{Z}$. $(P, \mathcal{N})$ is called a Canonical Number System (CNS) if each $A \in \mathcal{R}$ can be represented as

$$A = \sum_{j=0}^{k} a_j X^j, \quad a_j \in \mathcal{N}.$$

Examples of generalisations

- Akiyama *et al.*, $\frac{3}{2}$-problem,
- Kovács, CNS rings.

Settings

- $\mathcal{E}$ a commutative ring with identity,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,
- we will identify $X \in \mathcal{E}[X]$ with $X \in \mathcal{R}$,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,
- we will identify $X \in \mathcal{E}[X]$ with $X \in \mathcal{R}$,
- $m_\mathcal{N} : \mathcal{R} \to \mathcal{N}$ such that $A \equiv m_\mathcal{N}(A) \mod X$,

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,
- we will identify $X \in \mathcal{E}[X]$ with $X \in \mathcal{R}$,
- $m_{\mathcal{N}} : \mathcal{R} \to \mathcal{N}$ such that $A \equiv m_{\mathcal{N}}(A) \mod X$,
- $T_P : \mathcal{R} \to \mathcal{R}, A \mapsto \frac{A - m_{\mathcal{N}}(A)}{X}$.

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,
- we will identify $X \in \mathcal{E}[X]$ with $X \in \mathcal{R}$,
- $m_{\mathcal{N}} : \mathcal{R} \to \mathcal{N}$ such that $A \equiv m_{\mathcal{N}}(A) \mod X$,
- $T_P : \mathcal{R} \to \mathcal{R}, A \mapsto \frac{A - m_{\mathcal{N}}(A)}{X}$.

Settings

- $\mathcal{E}$ a commutative ring with identity,
- $P(X) = p_d X^d + \cdots + p_1 X + p_0 \in \mathcal{E}[X]$, $d \geq 1$,
- p_d no zero divisor,
- p_0 neither a unit nor a zero divisor, $\mathcal{E}/p_0$ finite,
- $\mathcal{R} = \mathcal{E}[X]/(P)$ the residue class ring,
- $\mathcal{N} \subset \mathcal{R}$ a set of representatives of $\mathcal{R}/(X)$,
- we will identify $X \in \mathcal{E}[X]$ with $X \in \mathcal{R}$,
- $m_{\mathcal{N}} : \mathcal{R} \to \mathcal{N}$ such that $A \equiv m_{\mathcal{N}}(A) \mod X$,
- $T_P : \mathcal{R} \to \mathcal{R}, A \mapsto \frac{A - m_{\mathcal{N}}(A)}{X}$.

Note that $\mathcal{R}/(X) \cong \mathcal{E}/p_0$.

X-ary representation

Definition

We call the triple $(\mathcal{R}, X, \mathcal{N})$ a digit system in $\mathcal{R}$.

X-ary representation

Definition

We call the triple $(\mathcal{R}, X, \mathcal{N})$ a digit system in $\mathcal{R}$.

Definition

For an $A \in \mathcal{R}$ we call $X_P(A) := \left(m_{\mathcal{N}}\left(T_P^n(A)\right)\right)_{n \in \mathbb{N}} \subset \mathcal{N}^\infty$ the X-ary representation. $X_P(A)$ is called periodic if it ends up periodically. $(\mathcal{R}, X, \mathcal{N})$ has the periodic representation property if $X_P(A)$ is periodic for all $A \in \mathcal{R}$.

X-ary expansion

Definition

Let $A \in \mathcal{R}$ and $X_P(A) = (a_n)_{n \in \mathbb{N}}$. If there exists an $l \in \mathcal{N}$ such that

$$A = \sum_{j=0}^{l} a_j X^j$$

we call this sum the finite X-ary expansion of A. $(\mathcal{R}, X, \mathcal{N})$ is said to have the finite expansion property if each $A \in \mathcal{R}$ has a finite X-ary expansion.

General results

Proposition

$A \in \mathcal{R}$ has a finite X-ary expansion if and only if $T_P^n(A) = 0$ for some $n \in \mathbb{N}$.

General results

Proposition

$A \in \mathcal{R}$ has a finite X-ary expansion if and only if $T_P^n(A) = 0$ for some $n \in \mathbb{N}$.

Proposition

The finite expansion property implies the periodic representation property.

Denote by $\mathcal{P}(\mathcal{R}, X, \mathcal{N})$ the set of purely periodic points:
$\mathcal{P}(\mathcal{R}, X, \mathcal{N}) = \{A \in \mathcal{R} | \exists n \geq 1 : T_P^n(A) = A\}$.

Denote by $\mathcal{P}(\mathcal{R}, X, \mathcal{N})$ the set of purely periodic points:
$\mathcal{P}(\mathcal{R}, X, \mathcal{N}) = \{A \in \mathcal{R} | \exists n \geq 1 : T_P^n(A) = A\}$.

Theorem

$(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property if and only if $(\mathcal{R}, X, \mathcal{N})$ has the periodic representation property, $0 \in \mathcal{P}(\mathcal{R}, X, \mathcal{N})$ and $|\mathcal{P}(\mathcal{R}, X, \mathcal{N})/T_P| = 1$.

Denote by $\mathcal{P}(\mathcal{R}, X, \mathcal{N})$ the set of purely periodic points:
$\mathcal{P}(\mathcal{R}, X, \mathcal{N}) = \{A \in \mathcal{R} | \exists n \geq 1 : T_P^n(A) = A\}$.

Theorem

$(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property if and only if $(\mathcal{R}, X, \mathcal{N})$ has the periodic representation property, $0 \in \mathcal{P}(\mathcal{R}, X, \mathcal{N})$ and $|\mathcal{P}(\mathcal{R}, X, \mathcal{N})/T_P| = 1$.

Theorem (Composition Theorem)

Let $(\mathcal{R}_1, X, \mathcal{N}_1)$, $(\mathcal{R}_2, X, \mathcal{N}_2)$ induced by the polynomials $P_1 \in \mathcal{E}[x]$ and $P_2 \in \mathcal{E}[x]$ and suppose both of them to have the finite expansion property. If $(|\mathcal{P}(\mathcal{R}_1, X, \mathcal{N}_1)|, |\mathcal{P}(\mathcal{R}_2, X, \mathcal{N}_2)|) = 1$. Then $(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property for $\mathcal{R} = \mathcal{E}[X]/(P_1 P_2)$ and

$$\mathcal{N} = \{d + eP_1 | d \in \mathcal{N}_1, e \in \mathcal{N}_2\}.$$

The P-lattice

Definition

Let $w_0 = p_d$, $w_k = Xw_{k-1} + p_{d-k}$ for $k = 1, \ldots, d-1$. We call the $\mathcal{E}$-submodule of $\mathcal{R}$ generated by the w_i the P-lattice of $\mathcal{R}$ and denote it by $\Lambda_P(\mathcal{R})$.

The P-lattice

Definition

Let $w_0 = p_d$, $w_k = Xw_{k-1} + p_{d-k}$ for $k = 1, \ldots, d-1$. We call the $\mathcal{E}$-submodule of $\mathcal{R}$ generated by the w_i the P-lattice of $\mathcal{R}$ and denote it by $\Lambda_P(\mathcal{R})$.

For $p_d = \pm 1$ we have $\Lambda_P(\mathcal{R}) = \mathcal{R}$. This is definitely NOT true for $p_d \neq \pm 1$.

The P-lattice

Definition

Let $w_0 = p_d$, $w_k = Xw_{k-1} + p_{d-k}$ for $k = 1, \ldots, d-1$. We call the $\mathcal{E}$-submodule of $\mathcal{R}$ generated by the w_i the P-lattice of $\mathcal{R}$ and denote it by $\Lambda_P(\mathcal{R})$.

For $p_d = \pm 1$ we have $\Lambda_P(\mathcal{R}) = \mathcal{R}$. This is definitely NOT true for $p_d \neq \pm 1$.

Theorem

Let $\mathcal{N} \subset \mathcal{E}$. $(\mathcal{R}, X, \mathcal{N})$ has the periodic representation property (the finite expansion property, resp.) if and only if each element of $\Lambda_P(\mathcal{R})$ has a periodic X-ary representation (a finite X-ary expansion, resp.).

Euclidean rings

Theorem

Suppose $\mathcal{E}$ to be Euclidean with value function $g : \mathcal{E} \to [0, \infty) \cup \{-\infty\}$ where $g(0) = -\infty$ and let $(\mathcal{R}, X, \mathcal{N})$ be a digit system satisfying $g(e) < g(p_0)$ for all $e \in \mathcal{N}$. If $(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property then $g(p_d) < g(p_0)$.

Polynomial rings over finite fields

Consider $\mathcal{E} = \mathbb{F}[y]$ to be the ring of polynomials (in y) over a finite field $\mathbb{F}$ and $\mathcal{N} = \{e \in \mathcal{E} | \deg_y(e) < \deg_y(p_0)\}$.

Polynomial rings over finite fields

Consider $\mathcal{E} = \mathbb{F}[y]$ to be the ring of polynomials (in y) over a finite field $\mathbb{F}$ and $\mathcal{N} = \{e \in \mathcal{E} | \deg_y(e) < \deg_y(p_0)\}$.

Theorem (Scheicher and Thuswaldner)

If $\deg_y(p_d) = 0$ *then* $(\mathcal{R}, X, \mathcal{N})$ *has the finite expansion property if and only if* $\deg_y(p_j) < \deg_y(p_0)$ *for all* $j \in \{1, \ldots, d-1\}$.

Polynomial rings over finite fields

Consider $\mathcal{E} = \mathbb{F}[y]$ to be the ring of polynomials (in y) over a finite field $\mathbb{F}$ and $\mathcal{N} = \{e \in \mathcal{E} | \deg_y(e) < \deg_y(p_0)\}$.

Theorem (Scheicher and Thuswaldner)

If $\deg_y(p_d) = 0$ *then* $(\mathcal{R}, X, \mathcal{N})$ *has the finite expansion property if and only if* $\deg_y(p_j) < \deg_y(p_0)$ *for all* $j \in \{1, \dots, d-1\}$.

Theorem

$(\mathcal{R}, X, \mathcal{N})$ *has the finite expansion property if and only if* $\deg_y(p_j) < \deg_y(p_0)$ *for all* $j \in \{1, \dots, d\}$.

CNS

Note

If $\mathcal{E} = \mathbb{Z}$, P monic and $\mathcal{N} = [0, p_0) \cap \mathbb{Z}$ then
$(P, \mathcal{N})$ is s CNS if and only if $(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property.

CNS

Note

If $\mathcal{E} = \mathbb{Z}$, P monic and $\mathcal{N} = [0, p_0) \cap \mathbb{Z}$ then
$(P, \mathcal{N})$ is s CNS if and only if $(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property.

Definition

Let $\mathcal{E} = \mathbb{Z}$ and $\mathcal{N} = [0, p_0) \cap \mathbb{Z}$. If $(\mathcal{R}, X, \mathcal{N})$ has the finite expansion property we call the pair $(P, \mathcal{N})$ a generalised canonical number system (GCNS).

Shift radix systems

Definition (Akiyama *et al.*, 2005)

Let $\mathbf{r} \in \mathbb{R}^d$ and define
$\tau_{\mathbf{r}} : \mathbb{Z}^d \rightarrow \mathbb{Z}^d, \mathbf{x} = (x_0, \ldots, x_{d-1}) \mapsto (x_1, \ldots, x_{d-1}, \mathbf{r}\mathbf{x})$.
$\tau_{\mathbf{r}}$ is called a shift radix system (SRS) if for all $\mathbf{x} \in \mathbb{Z}^d$ there exists an $n \in \mathbb{N}$ such that $\tau_{\mathbf{r}}^n(\mathbf{x}) = \mathbf{0}$.

Shift radix systems

Definition (Akiyama *et al.*, 2005)

Let $\mathbf{r} \in \mathbb{R}^d$ and define
$\tau_{\mathbf{r}} : \mathbb{Z}^d \rightarrow \mathbb{Z}^d, \mathbf{x} = (x_0, \ldots, x_{d-1}) \mapsto (x_1, \ldots, x_{d-1}, \mathbf{r}\mathbf{x})$.
$\tau_{\mathbf{r}}$ is called a shift radix system (SRS) if for all $\mathbf{x} \in \mathbb{Z}^d$ there exists an $n \in \mathbb{N}$ such that $\tau_{\mathbf{r}}^n(\mathbf{x}) = \mathbf{0}$.

Theorem (Akiyama *et al.*)

$P = x^d + p_{d-1}X^{d-1} + \cdots + p_1 X + p_0$ induces a CNS if and only if $(\frac{1}{p_0}, \frac{p_{d-1}}{p_0}, \ldots, \frac{p_1}{p_0})$ induces an SRS.

Shift radix systems

Definition (Akiyama *et al.*, 2005)

Let $\mathbf{r} \in \mathbb{R}^d$ and define
$\tau_{\mathbf{r}} : \mathbb{Z}^d \to \mathbb{Z}^d, \mathbf{x} = (x_0, \dots, x_{d-1}) \mapsto (x_1, \dots, x_{d-1}, \mathbf{r}\mathbf{x})$.
$\tau_{\mathbf{r}}$ is called a shift radix system (SRS) if for all $\mathbf{x} \in \mathbb{Z}^d$ there exists an $n \in \mathbb{N}$ such that $\tau_{\mathbf{r}}^n(\mathbf{x}) = \mathbf{0}$.

Theorem (Akiyama *et al.*)

$P = x^d + p_{d-1}X^{d-1} + \cdots + p_1 X + p_0$ *induces a CNS if and only if* $(\frac{1}{p_0}, \frac{p_{d-1}}{p_0}, \dots, \frac{p_1}{p_0})$ *induces an SRS.*

Theorem

$P = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_1 X + p_0$ *induces a GCNS if and only if* $(\frac{p_d}{p_0}, \frac{p_{d-1}}{p_0}, \dots, \frac{p_1}{p_0})$ *induces an SRS.*

Thanks

Thank you for your attention!
Děkuji!
Obrigado!
Köszönöm!
Merci!
Grazie!
Bedankt!
Sağol!
Danke!

The research was supported by the FWF, project S9610
The slides are (soon) available : www.palovsky.com
E-mail: me@palovsky.com