The Heritage of Alexey Kuz'min

05 июня 2017

Research areas

Alexey Kuz'min and his followers gained significant results in almost all areas of cryptography and connected threads of mathematics and physics

Boolean and q-ary functions

Error correcting codes

Linear recurrences over rings and modules

- let $P = GF(q)$, $Q = GF(q^n)$, $q = p^l$, where p is prime
- representation of $f : P^n \mapsto P$ by $F : Q \mapsto P$
- $\mathcal{A}$ is a class of approximating functions
  - $h : (Q, +) \mapsto (P, +)$ – all homomorphisms
  - $g : Q \mapsto P$, $g(x) = h(x^k)$
- reduced trace representation $F = tr_P^Q(\Phi)$, where $\Phi(x)$ is a uniquely defined polynomial of a special type

the most accurate generalization of results on parameters of bent-functions from the case $l = 1$ to the case $l > 1$ is obtained if instead of the non-linearity degree of a function one considers its binary non-linearity index (in the case $l = 1$ these parameters coincide)
if f is bent then $2 < ind(f) < \frac{nl}{2}$

- let $q = 2$, $Q = R^* \times V$, where $R = GF(q^{\frac{n}{2}})$, V is a cyclic group of order $q^{\frac{n}{2}} + 1$
- $F : Q \mapsto P$
- $N_a(F \mid V)$ denotes number of $x \in V$ satisfying equation $F(x) = a$

if for some d and function $H : V \mapsto P$ equalities $N_d(H \mid V) = q^{\frac{n}{2}-1} + 1$, $N_a(H \mid V) = q^{\frac{n}{2}-1}$ for $a \neq d$ hold then function $F : Q \mapsto P$ defined by equalities $F(0) = d$, $F(x) = H(x^{q^{\frac{n}{2}}-1})$ for $x \neq 0$ is hyperbent-function.

a lot of results obtained on the way of characterization of hyperbent-functions

- investigations of systematic code, dual code, McWilliams identity, parity-check matrix an the Hamming distance of a code
- comparison of properties of codes over modules and linear spaces
- description of codes by polylinear recurrences being the most efficient for systematic and Abelian group codes
- special role of quasi-Frobenius modules in code theory
- cyclic Hamming and BCH codes over an arbitrary primary module

Linear recurring sequences over rings and modules – research areas

- Linear recurrences can provide longer period in comparison with recurrences over fields
- Efficient implementation for specific rings (no need for field implementation)
- Challenging task from mathematical point of view – finite fields apparatus generally non-applicable

Linear recurring sequences over rings and modules – research areas

- Distribution of occurrences of elements, evaluation of periodic properties and linear complexity
- Injectivity of compressing maps on the set of sequences
- Generalisations: polylinear recurring sequences

Notations

- $\boldsymbol{R}$ – finite ring (risidue $\mathbb{Z}_{\boldsymbol{p^n}}$, Galois $\boldsymbol{GR(q^n, p^n), q = p^r}$)
- $\boldsymbol{u : \mathbb{N} \to R}$ – a sequence over $\boldsymbol{R}$
- $\boldsymbol{F(x)}$ – unitary polynomial over $\boldsymbol{R}$, $\boldsymbol{degF(x) = m}$, $\boldsymbol{T(F) = min\{t \in \mathcal{N} : F(x)|x^t - e\}}$ – a period of $\boldsymbol{F(x)}$,
- $\boldsymbol{F(x)}$ is primitive if $\boldsymbol{T(F) = (q^m - 1)p^{n-1}}$ for Galois ring
- $\boldsymbol{L_R(F)}$ – a set of all sequences with minimal polynomial $\boldsymbol{F(x)}$
- $\boldsymbol{u_s, s = 0, \ldots, n - 1}$ – $\boldsymbol{s}$-th coordinate sequence

The distribution of elements on cycles of linear recurrents over rings of residues, 1992

- Higher estimates for the number of occurrences of element of a ring $\mathbb{Z}_{p^n}$ (tuples of elements) depending on p and characteristic polynomial $G(x)$ (before – Knuth and Webb / Long for sequences of order 2)
- Condition for occurrence of every element of a ring ($degG(x) > p^n/p - 1$)

Further developments - Kuz'min et al.

- In the special case when the characteristic polynomial of linear recurring sequence is a monic basic irreducible polynomial, an upper bound for modulus of difference between the number of occurrences of r-tuples in the linear recurring sequence over Galois rings and uniform distributed sequence is obtained. Kuzmin, Kamlovskii, 2000

Intersections – a tool for study analytic properties of sequences over rings

- Developed together with A.Nechaev intersections became a widely used apparatus for study linear recurring sequences over rings and their coordinate sequences
- Intersection is a relation between elements of coordinate sequences of linear recurring sequence

Intersections – an example

For coordinate sequences of a primitive sequence $\boldsymbol{u \in L_R(G)}$ the following relations hold

- $\boldsymbol{(x^{\tau_s - 1} \ominus e) \otimes u_s = j u_0^{(1)}, s = 1, 2, ..., n-1, j = 1, 2, ..., p-1}$
- $\boldsymbol{(x^{\tau_s - 1} \ominus e)^k \otimes u_s^k = k!(u_0^{(1)})^k, s = 1, 2, ..., n-1, j = 1, 2, ..., p-1}$

$\boldsymbol{u^{(s)} = \Phi_s(x), x^{\tau_s} - e \equiv p^{s+1}\Phi_{s+1}(x) \ mod \ F(x)}$

Intersections – application

Injectivity of compressing map of linear recurring sequences over residue rings: can we construct a filtering generator over rings?

- Compressing map: a filtering function of the form $\Psi(x_0, \ldots, x_{n-1})$ which maps coordinate sequences to the output of filtering generator
- The question is whether it is possible to derive the initial state of the filtering generator from the output sequence?

State of the art

- Chinese school: Huang, Dai, Tian – a proof of injectivity of several types compressing map (a possibility of unique reconstruction of initial state)
- Kuz'min, Nechaev et al.: exact algorithms for reconstruction

Basic algorithm for reconstruction - Reconstruction of linear recurrent sequence over prime residue ring from its image, 2010

The initial vector of primitive linear recurring sequence $u \in L_R(F)$ over residue ring $\mathbb{Z}_{p^n}$ could be uniquely reconstructed from the sequence u_{n-1} with complexity $O(p^{\frac{m}{2}} + mp^n)$, given $O(mp^n)$ elements of u_{n-1} belonging to its subsequence of the length $(p^m - 1)p^{n-2} + m$.

Further developments – Kuz'min et al.

- wider classes of compressing maps (Kuz'min et al. 2010, 2011)
- wider classes of rings – Galois ring (Kuz'min, Nechaev, 2011)

Another view at compressing maps: periods and linear complexity

Let $F(x)$ - be a primitive polynomial over $\mathbb{Z}_{p^n}, p \geq 3, n \geq 2$, $degF(x) \geq 2$, $u \in L_R(F)$, v – is a compressing map such that $v(i) = \psi u_{n-1}(i), i \geq 0$. Then $T(v) \geq \frac{1}{2}T(u)$. $T(v) = \frac{1}{2}T(u)$ if

- $F(x)$ is not a strongly primitive
- $\psi(x - e) = \psi(-x)$
- u does not contain elements of the form $p^{n-1}\epsilon, \epsilon \neq 0(modp)$

Lower estimates for linear complexity of wide classes of coordinate sequences of primitive sequences over residue rings

Polylinear recurring sequences over rings and modules, Kuz'min, Nechaev, Kurakin

- R – finite ring
- ${}_RM$ – R - modulus
- $\mu : \mathbb{N}_0^k \to M$ - k-sequence over M, $\mu(z) = \mu(z_1, ..., z_k)$
- $\mathcal{R}_k = R[x_1, ..., x_k]$ – a ring of polynomials of k variables
- multiplication is defined as:

$$A(x)\mu = \nu, \nu(z) = \sum_{i \in \mathbb{N}_0^k} a_i \mu(z + i)$$

Polylinear recurring sequences over rings and modules, Kuz'min, Nechaev, Kurakin

$\boldsymbol{\mu}$ - is a $\boldsymbol{k}$-linear recurring sequence over $\boldsymbol{M}$ if $\boldsymbol{Ann\mu}$ – is a unitary ideal of $\boldsymbol{R[x_1, ..., x_k]}$

Example: 2-arithmetic progression

	0	1	2	...
0	α_0	$\alpha_0 + \alpha_1$	$\alpha_0 + 2\alpha_1$	...
1	$\alpha_0 + \alpha_2$	$\alpha_0 + \alpha_1 + \alpha_2$	$\alpha_0 + 2\alpha_1 + \alpha_2$	...
2	$\alpha_0 + 2\alpha_2$	$\alpha_0 + \alpha_1 + 2\alpha_2$	$\alpha_0 + 2\alpha_1 + 2\alpha_2$	...

Polylinear recurring sequences: research areas

- general investigation methodology
- construction techniques
- linear complexity description
- periodical characteristics
- distribution of occurrences of elements

Our hearts will always keep bright remembrance

The Heritage of Alexey Kuz'min is a remarkable part of Mathematics and Cryptology