On the reconstruction of a linear recurrence of maximal period over a Galois ring by its highest coordinate sequence.

A. S. Kuzmin (Moscow) kzmn@mail.ru

A. A. Nechaev (Moscow) nechaev@cnit.msu.ru

1 Galois rings

Remind that a Galois ring is a finite commutative ring R with identity e such that for some prime number p and natural number n the lattice of all ideals of the ring R is a chain of the length n of the following form:

$$R \rhd pR \rhd \ldots \rhd p^{n-1}R \rhd p^n R = 0.$$

In this situation $\operatorname{char} R = p^n$, a quotient ring $\overline{R} = R/pR$, called *top-factor* of R, is a field of $q = p^r$ elements and $|R| = q^n$. A Galois ring is defined uniquely up to isomorphism by its cardinality and characteristic and is denoted by $R = \mathrm{GR}(q^n, p^n)$. Most important examples:

$$\mathrm{GR}(p^n, p^n) = \mathbb{Z}_{p^n}, \quad \mathrm{GR}(q, p) = \mathrm{GF}(q).$$

A natural epimorphism $R \to \overline{R} = R/pR = \mathrm{GF}(q)$ is one of the important instrument in the investigation of different transformations over Galois rings. In all what follows we denote the image of element $a \in R$ or polynomial $G(x) \in R[x]$ under the epimorphisms $R \to \overline{R}$ or $R[x] \to \overline{R}[x]$ correspondingly by $\overline{a}, \ \ \overline{G}(x)$.

Any Galois ring $R = \mathrm{GR}(p^{rn}, p^n)$ has the following construction:

$$R \cong \mathbb{Z}_{p^n}[x] \ \ / \ \ G(x)\mathbb{Z}_{p^n}[x],$$

where $G(x) \in \mathbb{Z}_{p^n}[x]$ is any monic polynomial of the degree r such that $\overline{G}(x) \in \mathbb{Z}_p[x]$ is an irreducible polynomial.

2 Recurrences and polynomials of maximal period

Let $R = GR(q^n, p^n)$ be a Galois ring and $u : \mathbb{N}_0 \to R$ be a sequence over R: $u = (u(0), u(1), ..., u(i), ...)$. We call u *a linear recurring sequence (LRS) of order* m with a *characteristic polynomial* $F(x) = x^m - f_{m-1}x^{m-1} ... - f_0$ if $u(i+m) = f_{m-1}u(i+m-1) + ... + f_0 u(i), \quad i \in \mathbb{N}_0$.

Let us denote by $L_R(F)$ the family of all such sequences.

A *period* of $F(x)$ is defined as

$$T(F) = \min\{t \in \mathbb{N} : \quad \exists l \in \mathbb{N}_0 \quad F(x)|x^l(x^t - e)\}.$$

There are well-known that a period $T(u)$ of any LRS $u \in L_R(F)$ satisfies the relations:

$$T(u)|T(F), \quad T(F) \leq \tau p^{n-1}, \quad \text{where } \tau = q^m - 1.$$

If $F(x) \in R[x]$, $\deg F(x) = m$, $T(F) = \tau p^{n-1}$, $\tau = q^m - 1$, then $F(x)$ is called *polynomial of maximal period* (*MP-polynomial*) over the Galois ring $R = \mathrm{GR}(q^n, p^n)$ and an LRS $u \in L_R(F)$ such that $T(u) = T(F) = \tau p^{n-1}$ is called *LRS of maximal period* (*MP-LRS*) over R .

Theorem 1. *A reversible polynomial $F(x) \in R[x]$ of the degree m is an MP-polynomial if and only if $T(\overline{F}) = \tau = q^m - 1$ and*

$$x^\tau \overset{F}{\equiv} e + p\Phi(x), \quad \deg \Phi(x) < m, \quad \textit{where} \tag{1}$$

$$\begin{aligned} &\bar{\Phi}(x) \neq 0, \ \textit{if } p > 2, \ \textit{or } p = n = 2, \\ &\bar{\Phi}(x) \notin \{0, \bar{e}\} \ \textit{if } p = 2 < n. \end{aligned} \tag{2}$$

Let $F(x)$ be an MP-polynomial and $u \in L_R(F)$. Then u is an MP-LRS if and only if $\overline{u} \neq \overline{0}$.

3 Coordinate sets of a Galois ring

A subset $K \subseteq R$ is called a *coordinate set of the ring* R if $0 \in K$ and for any element $a \in R$ there exists a unique element $\varkappa(a) \in K$ such that $\overline{a} = \overline{\varkappa(a)}$. For such K every element $a \in R$ has a unique representation in the form

$$a = \varkappa_0(a) + p\varkappa_1(a) + \ldots + p^{n-1}\varkappa_{n-1}(a), \quad \varkappa_t(a) \in K,\ t \in \overline{0, n-1}. \tag{3}$$

We call (3) the *decomposition of the element a in the coordinate set K* (*K-decomposition of a*).

Main example of a coordinate set: *Techmüeller coordinate set*: $\Gamma(R) = \{\alpha \in R : \alpha^q = \alpha\}$. $\Gamma(R)$-decomposition of element $a \in R$ we call *Techmüeller decomposition.*

If $R = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, then the *p-ary coordinate set*

$$\delta(R) = \overline{0, p-1} = \{0, 1, \ldots, p-1\}$$

is also important. Let us note that $\Gamma(\mathbb{Z}_{p^n}) = \left\{0, 1, 2^{p^{n-1}}, \ldots, (p-1)^{p^{n-1}}\right\}$ and equality $\Gamma(\mathbb{Z}_{p^n}) = \overline{0, p-1}$ fulfils exactly if $n = 1$, or $p = 2$.

Proposition 1. *For any coordinate set K of a Galois ring R there exists a unique polynomial $\psi_K(x) \in R[x]$ with properties*

$$\psi_K(\Gamma(R)) = K, \;\; \deg \psi_K(x) \leq q - 1, \;\psi_K(x) \equiv x \pmod{pR}.$$

We call $\psi_K(x)$ the *interpolation polynomial of the coordinate set K.* Note that if $K = \Gamma(R)$ then $\psi_K(x) = x$.

Consider the p-ary decomposition of a number $t \in \mathbb{N}$:

$$t = t_0 + pt_1 + ... + p^k t_k, \quad t_0, ..., t_k \in \overline{0, p-1},$$

and define the *index of nonlinearity* of a monomial $lx^t \neq 0$ by

$$\operatorname{ind} lx^t = t_0 + ... + t_k, \quad \operatorname{ind} 0 = -\infty.$$

We define the *index of nonlinearity* $\operatorname{ind}\psi(x)$ of $\psi(x) \in R[x]$ as the maximum of indices of nonlinearity over all its monomials. Note that the interpolation polynomial $\psi_K(x)$ of any coordinate set K satisfies the relations $\deg \psi_K(x) \leq q-1$, $q = p^r$ and therefore

$$1 \leq \operatorname{ind}\psi_K(x) \leq (p-1)r. \tag{4}$$

4 Main problem and results

Let u be an LRS with a characteristic MP-polynomial $F(x) \in R[x]$, $\deg F(x) = m$. Consider some coordinate set K of the ring R and the K-coordinate decomposition of items $u(i)$ of LRS u:

$$u(i) = w_0(i) + pw_1(i) + \ldots + p^{n-1}w_{n-1}(i),$$
$$w_t(i) = \varkappa_t(u(i)) \in K,\ t \in \overline{0, n-1}. \quad (5)$$

We can correlate to u the coordinate sequences $w_0, \ldots, w_{n-1}$ over the field $(K, \oplus, \odot) = \mathrm{GF}(q)$, with operations:

$$\forall \alpha, \beta \in K: \quad \alpha \oplus \beta = \varkappa_0(\alpha + \beta),\ \ \alpha \odot \beta = \varkappa_0(\alpha \cdot \beta).$$

It is known that

$$T(u) = \tau p^{n-1} \iff T(w_{n-1}) = \tau p^{n-1}.$$

This motivates us to advance the following

Conjecture 1. *For any coordinate set K the sequence u can be uniquely reconstructed by the sequence w_{n-1}.*

This statement was proved earlier for

$$R = \mathbb{Z}_{p^n}, K = \overline{0, p-1}$$

(Kuzmin, Nechaev, Min-Qiang Huang, Zong-Duo Dai, 1992). In 2002 Weng-Feng Qi and Xuan-Yong Zhu have published the proof for the case

$$R = \mathrm{GR}(2^{rn}, 2^n), \quad K = \Gamma(R)$$

with some restriction on $F(x)$ (see below).

Here we prove that Conjecture 1 is true for an arbitrary Galois ring R with some restrictions on coordinate set K and polynomial $F(x)$.

Let us repeat some previous results.

A reversible polynomial $F(x)$ of the degree m over a Galois ring $\mathrm{GR}(q^n, p^n)$ is an MP-polynomial if and only if $T(\overline{F}) = \tau = q^m - 1$ and

$$x^\tau \overset{F}{\equiv} e + p\Phi(x), \quad \deg \Phi(x) < m, \quad \text{where} \tag{1}$$

$$\begin{aligned} &\bar{\Phi}(x) \neq 0, \text{ if } p > 2, \text{ or } p = n = 2, \\ &\bar{\Phi}(x) \notin \{0, \bar{e}\} \text{ if } p = 2 < n. \end{aligned} \tag{2}$$

If $F(x)$ be an MP-polynomial and $u \in L_R(F)$, then u is an MP-LRS if and only if $\overline{u} \neq \overline{0}$.

Any coordinate set K of the ring R has unique interpolation polynomial $\psi_K(x) \in R[x]$:

$$K = \psi_K(\Gamma(R)), \quad \psi_K(x) \equiv x \pmod{pR}, \qquad \operatorname{ind} \psi_K(x) \leq (p-1)r.$$

Main result of this talk:

Theorem 2. *If* $\operatorname{ind}\psi_K(x) \leq (p-1)$, *particularly if* $K = \Gamma(R)$, *then any MP-LRS* u *can be uniquely reconstructed by the highest coordinate sequence* w_{n-1} *from* K*-coordinate decomposition* (5)*:*

$$u(i) = w_0(i) + pw_1(i) + \ldots + p^{n-1}w_{n-1}(i), \quad w_t(i) \in K,\ t \in \overline{0, n-1}.$$

Note that Qi and Zhu (2002) have considered only the case when

$$R = \mathrm{GR}(2^{rn}, 2^n), \quad K = \Gamma(R),$$

$$x^\tau \overset{F}{\equiv} e + p\Phi(x),\ \ \deg\Phi(x) < m, \quad \deg\overline{\Phi}(x) > 0.$$

Namely this result we send firstly for the publication in the Proceedings of our conference.

However some later our student Kirill Gukov has find mistake in our proof. Our attempt to correct the proof before the deadline was unsuccessful. So we was in necessity send for publication the following impaired result, which is published in our Proceedings.

Theorem 3. *If* $\operatorname{ind}\psi_K(x) \leq (p-1)$*, particularly if* $K = \Gamma(R)$*, then any MP-LRS* u *can be uniquely reconstructed by the sequence* w_{n-1} *from* K*-coordinate decomposition* (5),

except possibly the case when

$$q > p = 2, \quad n > 3, \quad \deg \overline{\Phi}(x) = 0. \tag{6}$$

But now we have proof of the Theorem 2.

For $R = \mathbb{Z}_{p^n} = \mathrm{GR}(p^n, p^n)$ the equality $q = p$, i.e. $r = 1$ holds. Then any coordinate set K satisfy the condition

$$\operatorname{ind} \psi_K(x) \leq (p-1)$$

and condition $q > p = 2$ is false. This yields the

Corollary 1. *For any coordinate set K of a ring $R = \mathbb{Z}_{p^n}$ every MP LRS u over R can be uniquely reconstructed by coordinate sequence w_{n-1} from K-coordinate decomposition* (5).

Authors are grateful to D.Bylkov and K.Zukov for important remarks which made more precise the formulation of the main result.

References

[Kuzmin & Nechaev, 1992] A. S. Kuzmin, A. A. Nechaev, A construction of noise stable codes using linear recurrences over Galois rings, *Uspekhi Mat. Nauk*, **47** (5), 183–184, 1992.

[Kuzmin e.a., 2009] A. S. Kuzmin , G. B. Marshalko, A. A. Nechaev, Reconstruction of a linear recurrence over a primary residue ring, in: *Memoires in Discrete Mathematics*, vol. 12, Fizmatlit, Moscow, 2009, 155–194 (in Russian) to appear.

[Kurakin e.a., 1995] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechaev, Linear recurring sequences over rings and modules, *J. Math. Sci.*, **76** (6), 2793–2915, 1995.

[Nechaev] A. A. Nechaev, The cyclic types of linear substitutions over finite commutative rings, *Mat. Sb.*, **184** (3), 21–56, 1993.

[Huang & Dai, 1992] Min-Qiang Huang, Zong-Duo Dai, Projective maps of linear recurring sequences with maximal p-adic periods, *Fibonacchi Quart.*, **30**(2), 139–143, 1992.

[1] Xuan-Yong Zhu, Weng-Feng Qi, Compression mappings on primitive sequences over Z_{p^n}, *IEEE Trans. Inform. Theory*, **50** (10), 2442–2448, 2004.

[2] Xuan-Yong Zhu, Weng-Feng Qi, Further results of compressing maps on primitive sequences modulus odd prime number, *IEEE Trans. Inform. Theory*, **53** (8), 2985, 2007.

[3] Tian Tian, Wen-Feng Qi, Injectivity of compressing maps on primitive sequences over Z_{p^n}, *IEEE Trans. Inform. Theory*, **53** (8), 2960–2966, 2007.

[4] Zong-Duo Dai, Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials, *Journal of Cryptology*, **5** (4), 193–207, 1992.

[5] Weng-Feng Qi, Xuan-Yong Zhu, Compressing maps on primitive sequences over Z_{2^n} and its Galois extension, *Finite Fields and their applications*, **8** (4), 570–588, 2002.

[6] Weng-Feng Qi, *Compressing maps on primitive sequences over Z_{2n} and analysis of their derivate sequences*, Ph.D., Zhengzhou Inform. Eng. Univ., Zhengzhou, China, 1997.

[7] Weng-Feng Qi, Jun-Hui Yang, Jin-Jun Zhou, ML-sequences over rings Z_{2^n}, in *Advances in cryptology ASIACRYPT'98*, Berlin/Heidelberg: Springer-Verlag, **1514**, 315–325, 1998.