An criterion for annihilating ideals of linear recurring sequences over Galois rings

Peizhong Lu
Department of Computer Sciences
Fudan University
ppzlu@online.sh.cn

Mulan Liu
Institute of Systems Science
The Chinese Academy of Sciences

Abstract

Let R be a local Artin principal ideal ring, $R[x]$ the polynomial ring over R with indeterminate x. Let π be an element of R such that $\langle\pi\rangle$ is the unique maximal ideal of R. Let I be a zero-dimensional ideal of $R[x]$. In this paper we show that I is the annihilating ideal of a linear recurring sequence over R if and only if I satisfies the following formula

$$\dim_{R/\langle\pi\rangle} \frac{I : \langle\pi, d\rangle}{I} = \deg\, d,$$

for some squarefree polynomial d in $R/\langle\pi\rangle[x]$. The two sides of the formula can be feasibly computed by some typical algorithms from the theory of Gröbner bases. Our result is a solution of Nechaev's Open Problem..

Recently researches in algebraic coding theory over Galois rings, especially over Z_4, have received a great deal of attentions. Linear recurring sequences(LRS in short) over Galois rings are important contents to study in this area. For linear recurring sequences over a field, we have studied them well, but the cases over rings with zero divisors are much more complicated.

Let

$$\mathcal{M} = \left\{(a_i)_{i\in Z_+} \mid \text{for each } i \in Z_+,\, a_i \in R\right\}$$

be the set of all sequence over R. For each $j \in Z_+$, the j-translation of α, written ${}_j\alpha$, is defined by $({}_j\alpha)_i = \alpha_{i+j}$ for all $i \in Z_+$. Let $f(x) = \sum_i f_i x^i \in R[x]$ be a non-zero polynomial, where $i \in Z_+$. We define the action of $f(x)$ on α by $f(x)\alpha = \sum_i f_i \cdot_i \alpha$. It is easy to see that $\mathcal{M}$ is an $R[x]$-module with respect to the action of $R[x]$ on sequences. Let

$$\mathcal{A} = \{\alpha \in \mathcal{M} \mid \exists f(x) \in R[x],\, f(x)\alpha = 0\}. \tag{1}$$

Obviously, $\mathcal{A}$ is an $R[x]$-submodule of $\mathcal{M}$. We call an element of $\mathcal{A}$ a linear recurring sequence over R.

For any subset M of $\mathcal{M}$ and any ideal I of the ring $R[x]$, we define the sets

$$Zer_M(I) = \{\alpha \in M \,|\, f \cdot \alpha = 0, \text{ for each } f \in I\} \tag{2}$$

and

$$Ann_{R[x]}(M) = \{f \in R[x] \,|\text{for each } \alpha \in M,\ f \cdot \alpha = 0\}.$$

Especially, for a sequence α, $Ann_{R[x]}(\alpha)$ is the ideal consisting of all annihilators in the ring $R[x]$ and is called the **annihilating ideal** of α or the **characteristic ideal** of α.

Nechaev(1992) suggested the following open problem.

Nechaev′s Open Problem: *Let I be a monic ideal of $R[x]$. Deduce a criterion for the cyclicity of $R[x]$-module $Zer_{\mathcal{A}}(I)$ without using the primary decomposition of the ideal I.*

In this paper we are devoted to solve Nechaev′s Open Problem. Our main result is to present a formula to determine whether or not a given zero-dimensional ideal I of $R[x]$ is exactly an annihilating ideal of an LRS over R. This formula can also be used to characterize whether or not the module $Zer_{\mathcal{A}}(I)$ is a cyclic $R[x]$-module. Moreover, the formula is feasible to be computed by some typical algorithms from the theory of Gröbner bases.