数理解析研究所講究録 1375 巻 2004 年 8-14



# Log-ring size and value size of generators of subrings of polynomials over a finite field

Hidenosuke Nishio
西尾英之助 (元・京大理)
Iwakura Miyake-cho 204,
Sakyo-ku, Kyoto, 606-0022 Japan.
email: YRA05762@nifty.ne.jp

**Abstract**: In the paper we prove that

$$(*) \quad \log_q |\langle G\rangle| = |V(G)|,$$

where $G$ is any subset of a polynomial ring $Q[X]$ over a finite field $Q = GF(q)$ modulo $(X^q - X)$, $\langle G\rangle$ is the subring of $Q[X]$ generated by $G$ and $V(G)$ is the set of values of $G$. $|A|$ means the cardinality (size) of a set $A$. This research has its origin and gives another result in our study on the information dynamics of cellular automata where the cell state is a polynomial over a finite field. At the same time, it should be noticed that the equation (*) itself may serve as a powerful tool in the computer algebra—subring generation.

**Keywords**: polynomials over finite fields, subring, generator, cellular automaton

## 1 Preliminaries

This paper addresses an algebraic problem which arose in our study of the information dynamics of cellular automata, see the concluding remarks of [4]. However, its presentation here is self-contained and can be read without knowledge of the literature.

The problem is to investigate the structure of subrings of a polynomial ring $Q[X]$ modulo $(X^q - X)$ over $Q = GF(q), q = p^n$, where $p$ is a prime number and $n$ is a positive integer. Evidently $|Q| = q$. $Q[X]$ is considered to be the set of polynomial functions $\{g : Q \to Q\}$, which are uniquely expressed by the following polynomial form.

$$g(X) = a_0 + a_1X + \cdots + a_iX^i + \cdots + a_{q-1}X^{q-1},\ a_i \in Q,\ 0 \le i \le q-1. \quad (1)$$

It is easily seen that $|Q[X]| = q^q$. For any element $\alpha \in Q[X]$, we note that $\alpha^q - \alpha = 0$ and $p\alpha = 0$. As for the literature of finite fields and polynomials over them, we refer to the encyclopedia by Lidl and Niederreiter [3].

**Notation :** For a subset $G \subseteq Q[X]$, by $\langle G\rangle$ we mean the subring of $Q[X]$ which is generated by $G$. $G$ is called a generator set of $\langle G\rangle$. Every element of $G$ is called a generator of $\langle G\rangle$. For a ring, there may exist more than one generator sets. See Supplements below, where the general case of universal algebra is written, since the ring $R$ with identity element 1 is an algebra $\langle R, +, -, 0, \cdot, 1\rangle$.

It is an interesting topics to investigate the lattice structure (set inclusion) of subrings of $Q[X]$. Since we consider nontrivial subrings, the smallest subring is $Q$, while the largest one is $Q[X]$. In this paper we focus on the cardinality of subrings. The cardinality $|B|$ of an arbitrary subring $B \subseteq Q[X]$ is a power of $q$. For any $1 \le i \le q$, there exists a subring $B$ such that $|B| = q^i$, see Theorem (4) below. There can be more than one subrings having the same cardinality, see Example 3 below.

Now we are going to enter the main topics. First, we need to define the following two notions.

## 2 Log-ring size of $G$

Taking into account the fact that the cardinality of any subring of $Q[X]$ is a power of $q$, we define the *log-ring size* of $G$ by the following equation.

**Definition 1.** For any subset $G \subseteq Q[X]$, the *log-ring size* $\lambda(G)$ is defined by the following equation.

$$\lambda(G) = \log_q |\langle G\rangle| \tag{2}$$

Note that $1 \le \lambda(G) \le q$.

## 3 Value size of $G$

**Definition 2.** Suppose that a subset $G \subseteq Q[X]$ consists of $r$ polynomials: $G = \{g_1, g_2, ..., g_r : g_i \in Q[X], 1 \le i \le r\}$. Then an $r$-tuple of values $(g_1(a), g_2(a), ..., g_r(a))$ for $a \in Q$ is called the value vector of $G$ for $a$ and denoted by $G(a)$. Note that $G(a) \in Q^r$. The value set $V(G)$ of $G$ is defined by

$$V(G) = \{G(a) \mid a \in Q\}. \tag{3}$$

Finally we define the *value size* of $G$ by $|V(G)|$. Note that $1 \le |V(G)| \le q$.

When $G$ consists of one polynomial, say $G = \{g\}$, we simply denote $\langle g\rangle$ and $V(g)$ in stead of $\langle\{g\}\rangle$ and $V(\{g\})$, respectively.

## 4 Theorems

We state and prove the main theorem and one of its derivatives. The main theorem appeared without proof in the concluding remarks of our paper [4], page 416. It also gives another (much simpler) proof of Theorem 5.3 of the same paper as the special case of $|V(G)| = \lambda(G) = q$, which corresponds to the nondegeneracy and the completeness of a configuration.

**Theorem 3.** *For any subset $G \subseteq Q[X]$, the log-ring size is equal to the value size.*

$$\lambda(G) = \log_q |\langle G \rangle| = |V(G)|. \tag{4}$$

*Proof.* For given $G$ we assume that $m = q - |V(G)| > 0$ [1]. Then there are $m$ elements $c_1, c_2, .., c_m \in Q$ and a value vector $\gamma \in V(G)$ such that

$$G(c_i) = \gamma,\ 1 \leq i \leq m. \tag{5}$$

and

$$\gamma \neq G(a) \neq G(a') \neq \gamma \text{ for any } a \neq c_i, a' \neq c_i, 1 \leq i \leq m. \tag{6}$$

Such a $G$ is called $(c_1, c_2, ...c_m)$-degenerate. From the commutativity property of the substitution and the ring operations [4], it is seen that any polynomial function which is obtained from $(c_1, c_2, ...c_m)$-degenerate functions by ring operations is also $(c_1, c_2, ..., c_m)$-degenerate. Therefore,

$$\langle G \rangle = \{h \in Q[X] \mid h \text{ is } (c_1, c_2, ..., c_m) - degenerate\}. \tag{7}$$

On the other hand, from Equations (5) and (6), the number of all $(c_1, c_2, ..., c_m)$-degenerate polynomials turns out to be $q^{q-m} = q^{|V(g)|}$. Therefore we see,

$$|\langle G \rangle| = q^{|V(G)|}. \tag{8}$$

Taking $\log_q$ of both sides, we have the theorem. When $m = 0$, every values of $G$ are different, $G$ generates $Q[X]$ and therefore $|\langle G \rangle| = q^q$. So, taking $\log_q$ we have the theorem.

Using Theorem (3) we have the following result.

**Theorem 4.** *For any $1 \leq i \leq q$, there exits a subring $B$ such that $|B| = q^i$.*

*Proof.* Consider a function $h$ such that $|V(h)| = i$. For example, take a function $h$ such that

$$\begin{aligned} &h(a_0) = a_0, h(a_1) = a_1, h(a_2) = a_2, \cdots, \\ &h(a_{i-1}) = a_{i-1} = h(a_i) = h(a_{i+1}) = \cdots = h(a_{q-1}). \end{aligned} \tag{9}$$

Then by the interpolation formula given in Supplement below, we obtain a polynomial $g$ such that $g(c) = h(c)$, for any $c \in Q$. Therefore we see $|V(g)| = |V(h)|$. Then by Theorem (3) we have $|\langle g \rangle| = |V(g)| = |V(h)| = q^i$.

[1] In the information dynamics, $m$ is called the degree of degeneracy [4].

## 5 Polynomials in several indeterminates

Theorems (3) and (4) proved above can be generalized to the polynomial ring in several indeterminates $X_1, X_2, ..., X_n$.

Let $Q[X_1, X_2, ..., X_n]$ be the polynomial ring modulo $(X_1^q - X_1)(X_2^q - X_2)\cdots(X_n^q - X_n)$ over $Q$. The log-ring size and the value size of $G \subseteq Q[X_1, X_2, ..., X_n]$ are defined in the same manner as the one indeterminate case. Note, however, that $1 \leq \lambda(G) \leq q^n$ and $1 \leq |V(G)| \leq q^n$. Then we have the following theorems which can be proved in the same manner as the one variable case.

**Theorem 5.** *For any subset $G \subseteq Q[X_1, X_2, ..., X_n]$,*

$$\lambda(G) = \log_q |\langle G \rangle| = |V(G)|. \tag{10}$$

**Theorem 6.** *For any $1 \leq i \leq q^n$, there exits a subring $B$ such that $|B| = q^i$.*

## 6 Examples

**Example 1:** $Q = GF(3) = \{0, 1, 2\}$

$G_1 = \{a + bX\}$, where $b \neq 0$. $\langle G_1 \rangle = Q[X]$.
Since $|Q[X]| = q^q$, $\lambda(G_1) = q$

Generally, for an arbitrary $Q$, any polynomial of degree 1 generates $Q[X]$ and is called a permutation of $Q$. Note that $|V(a + bX)| = q$, since $Q$ is a field and $a + bc = a + bc'$ implies $c = c'$.

$G_2 = \{X^2\}$. We see that

$$\langle G_2 \rangle = \{0, 1, 2, X^2, 2X^2, 1 + X^2, 2 + X^2, 1 + 2X^2, 2 + 2X^2\} \neq Q[X].$$

So, $|\langle G_2 \rangle| = 9 = 3^2$ and $\lambda(G_2) = 2$. It is the only nontrivial subring of polynomials over GF(3). On the other hand we see $|V(X^2)| = 2$.

**Example 2:** $Q$=GF(4)=GF($2^2$)= $\{0, 1, \omega, 1 + \omega\}$. Note that $\omega^2 = 1 + \omega$, $(1 + \omega)^2 = \omega$ and $\omega(1 + \omega) = 1$. $2a = 0$ for any $a \in Q$.

$X^2$: $\langle X^2 \rangle = Q[X]$
$\lambda(X^2) = 4$. $|V(X^2)| = 4$.

$X^3$: $\langle X^3 \rangle = \{a + bX^3 : a, b \in Q\}$.
$|\langle X^3 \rangle| = 4^2$ $(\lambda(X^3) = 2)$. $|V(X^3)| = 2$.

$X + X^3$: $\langle X + X^3\rangle = \{a + bX + cX^3 : a, b, c \in Q\}$.
$|\langle X + X^3\rangle| = 4^3$ ($\lambda(X + X^3) = 3$). $|V(X + X^3)| = 3$.

**Example 3:** $Q$=GF(5)=$\{0, 1, 2, 3, 4\}$

We consider the following singleton subsets; $G_3 = \{X^4\}$, $G_4 = \{X^2\}$, $G_5 = \{X + X^3 + X^4\}$ and $G_6 = \{X^3\}$.
Then we have the following results on value size and log-ring size.

$G_3 = X^4 : \langle X^4\rangle = \{a + bX^4 : a, b \in Q\}$.
$|\langle X^4\rangle| = 5^2$ ( $\lambda(X^4) = 2$). On the other hand $|V(X^4)| = 2$.

$G_4 = X^2$:

$$\langle X^2\rangle = \{a + bX^2 + cX^4 : a, b, c \in Q\}. \tag{11}$$

$|\langle X^2\rangle| = 5^3$ ( $\lambda(X^2) = 3$). On the other hand $|V(X^2)| = 3$.

**Problem**: Show $|\langle X + X^3 + X^4\rangle| = 5^4$.
Also, show $|\langle 4X + 4X^2 + 2X^3 + X^4\rangle| = 5^4$.
Are they the same subring of cardinality $5^4$ ?
On the other hand $|V(X + X^3 + X^4)| = 4$.

$G_6 = X^3 : \langle X^3\rangle = Q[X]$, since $(X^3)^2 = X^2$ and $X^3 \cdot X^2 = X$ .
$\lambda(X^3) = 5$. It is seen that $|V(X^3)| = 5$.

$G_7 = X + X^2$: $|V(X + X^2)| = 3$. $|\langle G_7\rangle| = 3$ ?

$G_8 = G_4 \cup G_7 = \{X^2, X + X^2\}$: $V(G_8) = \{(0, 0), (1, 2), (4, 1), (4, 2), (1, 0)\}$.
So, $|V(G_8)| = 5$. On the other hand $\langle G_8\rangle = Q[X]$. So, $\lambda(G_8) = 5$.

It is clear that the subrings of a polynomial ring constitutes a lattice (set inclusion) structure. In order to calculate the complete diagram, even for small $q$, we need a computer software. However, as far as we know, there does not exist such a program that generates every subring of a polynomial ring over a finite field modulo $X^q - X$.

Here are shown partial inclusion relations of the above Example 3, $q = 5$.

$$Q \subset \langle X^4\rangle \subset \langle X^2\rangle \subset Q[X].$$

$$Q \subset \langle X + X^2\rangle \subset Q[X].$$

Note that $\langle X^2\rangle \neq \langle X + X^2\rangle$ and $\langle X^4\rangle$ is not included by $\langle X + X^2\rangle$.

In fact, from (11) we see that in any polynomial in $\langle X^2 \rangle$ the coefficient of the term $X^3$ is zero, while in $\langle X + X^2 \rangle$ we see for example $(X + X^2)^2 = X^2 + 2X^3 + X^4$.

# 7 Supplements

## 7.1 Interpolation formula

Given a function $h(x) : Q \to Q$, the following interpolation formula gives a unique polynomial function $f(x)$ over $Q$ such that $f(c) = h(c), \forall c \in Q$. In Chapter 5, page 369 of the encyclopedia by Lidl and Niederreiter [3], Equation (7.20) gives the interpolation formula for several indeterminates. Here we cite its one indeterminate version.

$$f(x) = \sum_{c \in Q} h(c)(1 - (x - c)^{q-1}) \tag{12}$$

By this formula we can compute the coefficients $a_i, 0 \leq i \leq q - 1$ in formula (1) from the value set of $h$, though inefficient.

## 7.2 Generators

A (universal) algebra [2] is a pair $\mathbf{A} = (A, O)$, where $A$ is a nonempty set called a universe and $O$ is a set of operations $f_1, f_2, ...$ on $A$. For a nonnegative integer $n$, an $n$-ary operation on $A$ is a function $f : A^n \to A$. A subuniverse of an algebra $\mathbf{A}$ is a subset of $A$ closed under all of the operations of $\mathbf{A}$. The collection of subuniverses of $\mathbf{A}$ is denoted by Sub( $\mathbf{A}$). For any subset $B$ of $A$, we define

$$\langle B \rangle^{\mathbf{A}} = \bigcap \{S \in Sub(\mathbf{A}) | B \subseteq S\}$$

called the ***subuniverse of* A *generated by* $B$**. If $\langle B \rangle^{\mathbf{A}} = A$, then we say that $B$ is a ***generating set for* A**.

**Classification:** According to Schmid [5], the elements of $\mathbf{A}$ is classified into three categories:

**(1) irreducibles:** elements that must be included in every generating set.
**(2) nongenerators:** elements that can be omitted from every generating set.
**(3) relative generators:** elements that play an essential role in at least one generating set.

This classification is closely related to the information contained by a polynomial in a configuration.

[2] For the universal algebra, the reader is referred to [2]

**Decision problems:** Bergman and Slutzki asked and answered the following questions [1] :

**(1)**: Does a given subset generate a given algebra ? Answer: **P**-complete.

**(2)**: What is the size of the smallest generating set of a given (finite) algebra ? Answer: **NP**-complete.

These results give an answer to the computational complexity problem whether a configuration is complete or not.

## 8 Acknowledgements

The main body of this research was carried out during my stay at Faculty of Informatics, University of Karlsruhe, September-October, 2003. The simulation program of CA[X] made by T. Saito was helpful in calculating subrings of $Q[X]$ given in Examples. Many thanks are due to them.

## References

1. Bergman, C., Slutzki, G.: Computational Complexity of Generators and Nongenerators in Algebra, *International Journal of Algebra and Computation*, **12**, 2002, 719–735.
2. Burris, S., Sankappanavar, H. P.: *A Course in Universal Algebra*, The millennium edition, Open website, 2000.
3. Lidl, R., Niederreiter, H.: *Finite Fields*, Second edition, Cambridge University Press, 1997.
4. Nishio, H., Saito, T.: Information Dynamics of Cellular Automata I: An Algebraic Study, *Fundamenta Informaticae*, **58**, 2003, 399–420.
5. Schmid, J.: Nongenerators, genuine generators and irreducibles, *Heuston Journal of Mathematics*, **25**, 1999, 405–416.