数理解析研究所講究録
第2051巻 2017年 64-69

A Note on Idempotent Monomial Clones — Two is Strong; One is Weak —

Hajime Machida *　　Jovanka Pantović †　　Csaba Szabó ‡

Tokyo, Japan　　Novi Sad, Serbia　　Budapest, Hungary

Abstract

Clones of polynomials are considered over Galois field GF(k). In particular, the class of clones generated by 2-variable idempotent polynomials is the target of our study. Our results include that the clone generated by $x^2\,y^{k-2}$ is the largest among all such clones and the clone generated by xy^{k-1} is the smallest among all such clones. Hence, observing the exponent of one variable, two is strong and one is weak.

Keywords: clone; monomial clone; lattice of clones † ‡

1 Preliminaries

Let $k > 1$ be fixed and $E_k = \{0, 1, \ldots, k-1\}$. Denote by $\mathcal{O}_k^{(n)}$ for $n \geq 1$ the set of n-variable functions defined over E_k, that is, the set of maps from E_k^n into E_k. Also, $\mathcal{O}_k$ denotes the set of functions defined over E_k, i.e., $\mathcal{O}_k = \bigcup_{n=1}^{\infty} \mathcal{O}_k^{(n)}$. A special class of functions is the set $\mathcal{J}_k$ of *projections* e_i^n for any $n > 0$ and $1 \leq i \leq n$, where e_i^n is the function in $\mathcal{O}_k^{(n)}$ which always takes the value of the i-th variable.

A *clone* over E_k is a subset C of $\mathcal{O}_k$ which is closed under (functional) composition and includes $\mathcal{J}_k$. The set of clones over E_k forms a lattice with respect to inclusion and is denoted by $\mathcal{L}_k$. It is well-known that the lattice $\mathcal{L}_k$ for $k > 2$ has the cardinality of the continuum and its structure is extremely complex.

For arbitrary field K and a positive integer n, an (n-variable) *polynomial* over K is a finite sum of terms, that is,

$$\sum_{0 \leq i_1 \leq e_1, \ldots, 0 \leq i_n \leq e_n} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

for some $e_1, \ldots, e_n \in \mathbf{N}$ and $a_{i_1, \ldots, i_n} \in K$ for each n-tuple $(i_1, \ldots, i_n)$ in the specified range. As a special case, an (n-variable) *monomial* over K is an n-variable polynomial consisting of one term, i.e.,

$$a\, x_1^{i_1} \cdots x_n^{i_n}$$

for some $a \in K$ and $i_1, \ldots, i_n \in \mathbf{N}$.

*machida.zauber@gmail.com　†pantovic@uns.ac.rs　‡ csaba@cs.elte.hu

For a prime power k, i.e., $k = p^e$ for a prime p and a positive integer e, let us introduce the structure of a finite field into E_k, that is, we treat E_k as the Galois field $\mathrm{GF}(k)$. It is well-known that any n-variable function $f(x_1, \ldots, x_n)$ defined over $\mathrm{GF}(k)$ is uniquely expressed as a polynomial over $\mathrm{GF}(k)$. The following is a basic property of a finite field.

Property 1: For every $x \in \mathrm{GF}(k)$ it holds that $x^k = x$.

Hence, we have:

Property 2: An n-variable monomial m over $\mathrm{GF}(k)$, for $n > 0$, is expressed as $ax_1^{r_1} \cdots x_n^{r_n}$ for some $a \in \mathrm{GF}(k)$ and integers $r_1, \ldots, r_n$ with $0 < r_1, \ldots, r_n < k$.

For a subset S of $\mathcal{O}_k$, the clone *generated* by S is the smallest clone containing S and denoted by $\langle S \rangle$. When $S = \{f\}$, the clone $\langle S \rangle$ is denoted by $\langle f \rangle$. A monomial clone is defined as follows.

Definition 1.1 *A clone C over E_k is a* monomial clone *if C is generated by some monomial m over E_k, i.e., $C = \langle m \rangle$.*

The study of monomial clones is partly motivated by the following property. The proof is immediate as any polynomial which is not a monomial cannot be produced from monomials by means of composition.

Lemma 1.1 *Let C be a monomial clone over E_k. If C is minimal in the set of monomial clones then C is a minimal clone (in $\mathcal{L}_k$).*

In the rest of the paper we consider a limited class of monomials and monomial clones generated by them.

2 Idempotent Monomial Clones

An n-variable function f defined over E_k is said to be *idempotent* if f satisfies $f(a. \ldots, a) = a$ for all a in E_k. Let $m = x_1^{i_1} \cdots x_n^{i_n}$ be an n-variable monomial with coefficient 1 over $\mathrm{GF}(k)$. Evidently (by Property 1), m is *idempotent* if and only if $\sum_{j=1}^{n} i_j \equiv 1 \pmod{k-1}$. (We abuse the term idempotent for polynomials in an obvious way.)

Throughout the rest of the paper, we consider 2-variable idempotent monomials over E_k and monomial clones generated by them. Hereafter, by a monomial clone we shall mean a monomial clone generated by a 2-variable idempotent monomial. Let us denote by $\mathcal{M}_k$ the set of such monomial clones over E_k.

2.1 Monomials $x^s y^t$

As was stated above, we consider 2-variable monomials $x^s y^t$ for $0 < s, t < k$ with the additional condition $s + t = k$. (For convenience we use x and y, instead of x_1 and x_2, for the variable symbols.) Clearly, $s+t = k$ is an equivalent condition for $x^s y^t$ to be idempotent when the exponents s and t satisfy $0 < s, t < k$.

Note: If m is a monomial which generates a *non-unary minimal clone* (in $\mathcal{L}_k$) then, clearly, (1) m must be a 2-variable monomial $x^s y^t$ and (2) the condition $s+t = k$ must be satisfied,

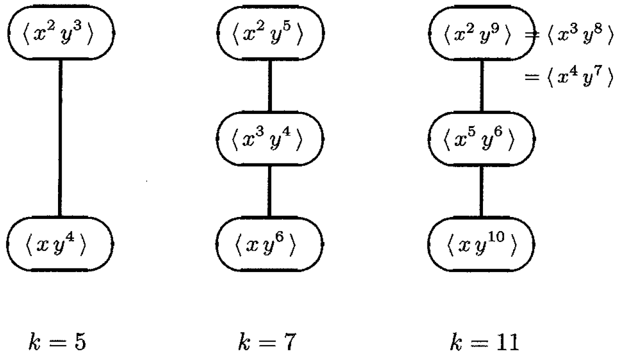


Figure 1: Monomial clones for $k = 5, 7, 11$

since $\langle x^s\, y^t \rangle$ does not contain any non-trivial unary functions.

The next lemma shows that the condition "$s + t = k$" on the exponents is *preserved* by composition. The proof is straightforward.

Lemma 2.1 *For integers u, v satisfying $0 < u, v < k$, if $x^u\, y^v$ is obtained from $x^s\, y^t$ (together with $\mathcal{J}_k$) by composition, i.e., $x^u\, y^v \in \langle x^s\, y^t \rangle$, then we have $u + v = k$.*

Some easy consequences are presented.

Lemma 2.2 *Let k be a prime power. For clones on* GF(k) *we have the following.*

(1) $\langle x\, y^{k-1} \rangle \subseteq \langle x^2\, y^{k-2} \rangle$ (2) $\langle x^4\, y^{k-4} \rangle \subseteq \langle x^3\, y^{k-3} \rangle$

Proof (i) From

$$(k-2)^2 \quad = \quad ((k-1)-1)^2 \;\equiv\; 1 \pmod{k-1}$$

it follows that $x^2(x^2 y^{k-2})^{k-2} = x^{k-1}y$.

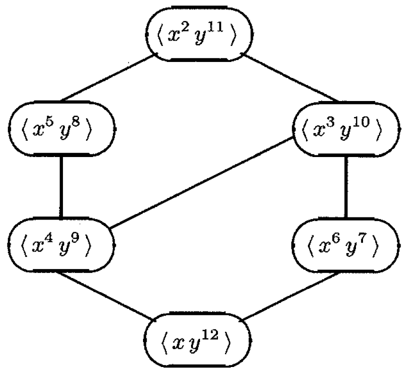
(ii) Similarly,

$$(k-3)^2 \quad = \quad ((k-1)-2)^2 \;\equiv\; 4 \pmod{k-1}$$

implies $x^3(x^3 y^{k-3})^{k-3} = x^{k-4}y^4$. □

3 Two is strong; One is weak

In Figures 1 and 2 the set $\mathcal{M}_k$ of the monomial clones is shown for the cases $k = 5$, 7, 11 and 13. An observation we get from these diagrams is the following (where two and one refer the exponents of one variable): Two is strong and one is weak !



$k = 13$

Figure 2: Monomial clones for $k = 13$

3.1 Two is strong

Proposition 3.1 *For any prime power $k > 1$ and any $0 < s < k$, it holds that*

$$\langle x^s y^{k-s} \rangle \subseteq \langle x^2 y^{k-2} \rangle.$$

In other words, $\langle x^2 y^{k-2} \rangle$ is the largest clone in $\mathcal{M}_k$.

Proof We shall prove $x^s y^{k-s} \in \langle x^2 y^{k-2} \rangle$ for any $0 < s < k$ by induction on s.
Basis: The monomial with $s = 1$, i.e., xy^{k-1}, is obtained from $x^2 y^{k-2}$ in the following way.

$$y^2 (y^2 x^{k-2})^{k-2} = x^{(k-2)^2} y^{2k-2} = xy^{k-1}$$

Thus we have $x^s y^{k-s} \in \langle x^2 y^{k-2} \rangle$ for $s = 1, 2$.

Inductive Step: For any $1 < t < \lfloor \frac{k}{2} \rfloor$, we obtain $x^{2t-1} y^{k-2s+1}$ and $x^{2t} y^{k-2s}$ from $x^t y^{k-t}$ and $x^2 y^{k-2}$ as shown below.

$$\begin{cases} (x^t y^{k-t})^2 x^{k-2} & = & x^{2t+k-2} y^{2k-2t} & = & x^{2t-1} y^{k-2t+1} \\ (x^t y^{k-t})^2 y^{k-2} & = & x^{2t} y^{3k-2t-2} & = & x^{2t} y^{k-2t} \end{cases}$$

This completes the proof. □

3.2 One is weak

Lemma 3.2 *The clone $\langle xy^{k-1} \rangle$ is minimal in $\mathcal{M}_k$.*

Proof For any monomial m in $\langle xy^{k-1} \rangle \setminus \mathcal{J}_k$, it is easy to verify that $xy^{k-1} \in \langle m \rangle$. This shows the minimality of $\langle xy^{k-1} \rangle$ in $\mathcal{M}_k$. □

Now a question arises, which we shall call Question A.

Question A: Is the clone $\langle xy^{k-1} \rangle$ uniquely minimal in $\mathcal{M}_k$? That is to say, is it true that $\langle xy^{k-1}\rangle \subseteq \langle x^s y^{k-s}\rangle$, i.e.,

$$xy^{k-1} \in \langle x^s y^{k-s}\rangle$$

holds for any prime power $k > 1$ and any $0 < s < k$?

Remark: It may happen that $\langle x^s y^{k-s}\rangle = \langle xy^{k-1}\rangle$ for some $s > 1$, in which case $\langle x^s y^{k-s}\rangle$ may also be said to be minimal in $\mathcal{M}_k$. What we want to know is whether $\langle x^s y^{k-s}\rangle$ for $2 \leq s < k$ is not minimal in $\mathcal{M}_k$ if $\langle x^s y^{k-s}\rangle$ is distinct from $\langle xy^{k-1}\rangle$.

3.3 Partial results Concerning Question A

Lemma 3.3 *Let $k = 2h+1$. Then $xy^{k-1} \in \langle x^h y^{k-h}\rangle$.*

Proof We get

$$(x^h y^{h+1})^h (y^h x^{h+1})^{h+1} \;=\; x^{h^2+(h+1)^2} y^{2h(h+1)} \;=\; xy^{2h} \;=\; xy^{k-1}$$

since $2h = k-1$. □

Lemma 3.4 *For $k > 2$ and $1 < a < k$, if there exists $e > 1$ satisfying*

$$\text{(i)}\;\; a^e \equiv 1 \pmod{k-1} \quad \textit{or} \quad \text{(ii)}\;\; a^e \equiv a \pmod{k-1}$$

then

$$xy^{k-1} \in \langle x^a y^{k-a}\rangle$$

Proof Since (ii) follows from (i), it suffices to show the result under the condition (ii). However, in order to enjoy a kind of symmetry in the proof we present the proof separately.

(i) By repeating substitution of $x^a y^{k-a}$ into x e times, we obtain:

$$((\cdots((x^a y^{k-a})^a y^{k-a})^a \cdots)^a y^{k-a})^a y^{k-a} \;=\; x^{a^e} y^* \;=\; xy^{k-1}$$

(ii) Similarly, we have:

$$\begin{aligned} ((\cdots((x^a y^{k-a})^a y^{k-a})^a \cdots)^a y^{k-a})^a x^{k-a} &= x^{a^e+(k-a)} y^* \;=\; x^{a+(k-a)} y^* \\ &= x^k y^{k-1} \;=\; xy^{k-1} \end{aligned}$$

Here the symbol * put on y designates a suitable exponent. □

Note that the condition (i) in Lemma 3.4 is equivalent to saying that a and $k-1$ are coprime, i.e., $\mathrm{GCD}(a, k-1) = 1$.

3.4 One is Provably Weak

We answer Question A affirmatively. The next lemma plays a key rôle in the proof.

Lemma 3.5 *For any $k > 0$ and $s \in E_k$ there exists $n > 0$ satisfying*

$$s^n \equiv (s^n)^2 \pmod{k-1}.$$

Proof Since k is finite, there exist $i > 0$ and $p > 0$ such that $s^i \equiv s^{i+p} \pmod{k-1}$. This obviously implies $s^i \equiv s^{i+rp} \pmod{k-1}$ for any $r > 0$. Take an integer $c > 0$ which satisfies $cp \geq i$ (e.g., $c = \lceil i/p \rceil$) and let $a = cp - i$. Then, we have:

$$\begin{aligned} s^{i+a} &\equiv s^{i+cp+a} && \pmod{k-1} \\ &\equiv s^{2i+2a} && \pmod{k-1} \\ &\equiv (s^{i+a})^2 && \pmod{k-1} \end{aligned}$$

Let $n = i + a$. Then n has the required property. □

Proposition 3.6 *For any prime power $k > 1$ and all $0 < s < k$, it holds that*

$$\langle xy^{k-1} \rangle \subseteq \langle x^s y^{k-s} \rangle,$$

that is, $\langle xy^{k-1} \rangle$ is uniquely minimal in $\mathcal{M}_k$.

Proof We show $xy^{k-1} \in \langle x^s y^{k-s} \rangle$ for any $0 < s < k$. According to Lemma 3.5 there exists $n > 0$ such that $s^n \equiv (s^n)^2 \pmod{k-1}$. Denote s^n by t.

Thus, t satisfies $t^2 \equiv t \pmod{k-1}$ and $x^t y^{k-t} \in \langle x^s y^{k-s} \rangle$. Now, from $x^t y^{k-t}$ construct a monomial

$$(x^t y^{k-t})^t x^{k-t} = x^{t^2-t+1} y^{t(k-t)}.$$

Since $t^2 - t \equiv 0 \pmod{k-1}$, we have

$$x^{t^2-t+1} y^{t(k-t)} = xy^{k-1},$$

from which it follows that $xy^{k-1} \in \langle x^t y^{k-t} \rangle$. Together with $x^t y^{k-t} \in \langle x^s y^{k-s} \rangle$, we conclude that $xy^{k-1} \in \langle x^s y^{k-s} \rangle$. □

Note: Some of the contents presented in this article appeared in [MP17].

References

[MP17] Machida, H. and Pantović, J., Three Classes of Closed Sets of Monomials, *Proceedings 47th International Symposium on Multiple-Valued Logic*, IEEE, 2017, 100-105.