数理解析研究所講究録
1489巻 2006年 261-264

Polynomials Generating Minimal Clones on a Finite Field

町田 元 (Hajime Machida)
一橋大学 (Hitotsubashi University)
machida@math.hit-u.ac.jp

1 Introduction

Let A be a fixed set with k elements where $k > 1$. For a positive integer n let $\mathcal{O}_A^{(n)}$ be the set of all n-ary operations on A, that is, maps from A^n into A, or n-variable functions on A, and let

$$\mathcal{O}_A = \bigcup_{n=1}^{\infty} \mathcal{O}_A^{(n)}.$$

Denote by $\mathcal{J}_A$ the set of all **projections** e_i^n, $1 \le i \le n$, over A where e_i^n is defined by

$$e_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i$$

for every $(x_1, \ldots, x_n) \in A^n$.

In this paper we consider only the case where A is a finite set. For simplicity, and without losing generality, let

$$A = \{0, 1, \ldots, k-1\}$$

for $k > 1$. An important factor about the set A is the number of the elements in A and we often write E_k instead of A when $|A| = k$. Also, write $\mathcal{O}_k^{(n)}$, $\mathcal{O}_k$ and $\mathcal{J}_k$ instead of $\mathcal{O}_A^{(n)}$, $\mathcal{O}_A$ and $\mathcal{J}_A$, respectively.

Definition 1.1 *A subset C of $\mathcal{O}_k$ is a* **clone** *on E_k if the following conditions are satisfied:*

(i) *C contains $\mathcal{J}_k$.*
(ii) *C is closed under (functional) composition.*

The set of all clones on E_k is denoted by L_k. The set L_k ordered by inclusion is called the **lattice of clones** *on E_k and is denoted by $\mathcal{L}_k$.*

The structure of $\mathcal{L}_2$ is completely known by E. Post ([Po41]). However, the structure of $\mathcal{L}_k$ for every $k \ge 3$ is extremely complex and at present mostly unknown. The cardinality of the lattice of clones is known for each $k \ge 2$: $|\mathcal{L}_2| = \aleph_0$ ([Po41]) and $|\mathcal{L}_k| = 2^{\aleph_0}$ for $3 \le k < \aleph_0$ ([IM59]).

Maximal clones and minimal clones are defined as follows:

Definition 1.2 *A clone C is a* **maximal clone** *if it is a co-atom of $\mathcal{L}_k$. In other words, C is a maximal clone if it satisfies the following conditions:*

(i) *$C \subset \mathcal{O}_k$.*
(ii) *For any $C' \in \mathcal{L}_k$, $C \subset C' \subseteq \mathcal{O}_k$ implies $C' = \mathcal{O}_k$.*

Definition 1.3 *A clone C is a* **minimal clone** *if it is an atom of $\mathcal{L}_k$. In other words, C is a minimal clone if it satisfies the following conditions:*

(i) *$\mathcal{J}_k \subset C$.*
(ii) *For any $C' \in \mathcal{L}_k$, $\mathcal{J}_k \subseteq C' \subset C$ implies $C' = \mathcal{J}_k$.*

Maximal clones are completely known by I. G. Rosenberg [Ro70]. They are characterized in terms of relations. In contrast to maximal clones, the problem of determining all minimal clones is still open, except for $k = 2$ and 3.

The problem of determining all minimal clones for every $k > 3$ is now generally recognized as one of the most challenging problems in clone theory. Quite a few papers have been published in connection to this problem and many of them contain nice and interesting results. However, one may see these results only to show the difficulty of this problem.

In this paper, we present a proposal to look at this problem from a new point of view. (See also [MP06].) We consider only the cases where k is a power of some prime number, i.e., $k = p^e$ for some prime p and $e \geq 1$. For such k, we may incorporate the algebraic structure of a *field* in the base set E_k. This can be done without loss of generality for our purpose. Now the set E_k is viewed as a Galois field.

$$E_k = \mathrm{GF}(k) = \{0, 1, \ldots, k-1\}$$

Then, consider an operation $f \in \mathcal{O}_k^{(n)}$ as a polynomial (in a usual sense) on a finite field E_k. Our task is to extract some nice properties which a polynomial must satisfy in order to be a generator of a minimal clone.

As an initial stage of this study, we discuss in this paper the relatively easily handled cases: The case where polynomials are linear and the case where polynomials are monomials. We show that, for every prime k, (i) linear function $ax + (k - a + 1)y$ is minimal for any $1 < a < k$ and (ii) monomial xy^{k-1} is a unique monomial which is minimal.

2 Minimal Clones

For $F \subseteq \mathcal{O}_k$, $\langle F \rangle$ denotes the clone generated by F, that is, $\langle F \rangle$ is the least clone containing F. When F is a sigleton, i.e., $F = \{f\}$, $\langle F \rangle$ is simply denoted by $\langle f \rangle$.

Lemma 2.1 *A minimal clone is generated by a single function. That is, for any minimal clone $C \in \mathcal{L}_k$ there exists $f \in \mathcal{O}_k$ such that $C = \langle f \rangle$.*

Complete list of minimal clones is known only for $k = 2$ and 3. However, we have the *type theorem* of minimal clones due to I. G. Rosenberg.

Definition 2.1 *An function f on E_k is* **minimal** *if* (i) *it generates a minimal clone and* (ii) *every function from $\langle f \rangle$ whose arity is smaller than the arity of f is a projection.*

Theorem 2.2 ([Ro86]) *Every minimal function belongs to one of the following five types:*

(1) *Unary functions f on E_k such that either* (i) *f^2 $(= f \circ f) = f$ or* (ii) *f is a permutation of prime order p (i.e., $f^p = id$).*

(2) *Idempotent binary functions; i.e., $f \in \mathcal{O}^{(2)}$ such that $f(x, x) = x$ for every $x \in E_k$.*

(3) *Majority functions; i.e., $f \in \mathcal{O}^{(3)}$ such that $f(x, x, y) = f(x, y, x) = f(y, x, x) = x$ for every x, $y \in E_k$.*

(4) *Semiprojections; i.e., $f \in \mathcal{O}^{(n)}$ $(3 \leq n \leq k)$ such that there exists i $(1 \leq i \leq n)$ satisfying $f(a_1, \ldots, a_n) = a_i$ whenever $a_1, \ldots, a_n \in E_k$ are not pairwise distinct.*

(5) *If $k = 2^m$, the ternary functions $f(x, y, z) := x + y + z$ where $\langle E_k; + \rangle$ is an elementary 2-group (i.e., the additive group of an m-dimensional vector space over GF(2)).*

Corollary 2.3 *The number of minimal clones is finite for every $k > 1$.*

For $k = 3$, B. Csákány determined all minimal clones by listing minimal functions generating them ([Cs83]).

3 Minimal Clones on a Finite Field

In this section, let k be a prime and $(E_k; +, \cdot)$ be a finite field (Galois field). We consider only idempotent binary functions (Item (2) in Theorem 2.2). Over a field E_k, a function $f \in \mathcal{O}_k^{(2)}$ can be expressed as

$$f(x, y) = \sum_{0 \leq i, j < k} a_{ij} x^i y^j$$

where $a_{ij} \in E_k$ for $0 \leq i, j < k$. Note that the operations $+$ and $\cdot$ are the operations performed over $\mathbf{Z}$ mod k. Also, note that $x^k = x$ for every $x \in E_k$.

3.1 Conjecture on Linear Functions

First, consider linear functions generating minimal clones.

Lemma 3.1 *Let $f(x,y) = ax + by + c$ for some $a, b, c \in E_k$. If f is idempotent then $a + b \equiv 1 \pmod{k}$ and $c = 0$.*

Observation 1:

(i) For $k = 3$, $2x + 2y$ is minimal.

(ii) For $k = 5$, $2x + 4y$ and $3x + 3y$ are minimal, which generate the same minimal clone.

(iii) For $k = 7$, $2x+6y$, $3x+5y$ and $4x+4y$ are minimal, which generate the same minimal clone.

(iv) For $k = 11$, $ax + by$ is minimal for all $1 < a, b < 11$ such that $a + b = 12$. All generate the same minimal clone.

This observation leads us to establish the following conjecture.

Conjecture 1: For any prime k, linear function $ax + (k - a + 1)y$ is minimal for any $1 < a < k$.

3.2 Conjecture on Monomials

Secondly, we shall consider monomials, i.e., polynomials consisting of a single term. We assume without loss of generality that a monomial is of the form $cx^s y^t$ where $1 \leq s \leq t < k$.

Lemma 3.2 *Let $f(x,y) = cx^s y^t$ for some $s, t \in \mathbf{N}$ and some $c \in E_k$. If f is idempotent then $c = 1$.*

Lemma 3.3 *Let $f(x,y) = x^s y^t$ for some $s, t \in \mathbf{N}$. If f is idempotent then $s + t = k$.*

Proof This follows from the equation $x^k = x$. □

Proposition 3.4 *For any prime k, $f(x,y) = x\,y^{k-1}$ is minimal.*

Proof We can readily verify, e.g., $f(f(x,y),y) = f(x,y)$, $f(f(y,x),y) = f(x,y)$, $f(x, f(x,y)) = f(x,y)$, etc., which justify the assertion of Proposition. □

Observation 2:

(i) For $k = 3$, xy^2 is the only monomial which is minimal.

(ii) For $k = 5$, xy^4 is the only monomial which is minimal.

(iii) For $k = 7$, xy^6 is the only monomial which is minimal.

(iv) For $k = 11$, xy^{10} is the only monomial which is minimal.

From this observation we are lead to conjecture the following.

Conjecture 2: Let k be a prime. Among monomials $x^s y^t$, $1 \leq s \leq t < k$, the monomial $x\,y^{k-1}$ is the only monomial which is minimal.

3.3 Results on Linear Functions

Due to Á. Szendrei, Conjecture 1 is known to hold (Personal communication).

Theorem 3.5 *For any prime k, linear function $ax + (k - a + 1)y$ is minimal for any $1 < a < k$. Moreover, all such linear functions generate the same minimal clone.*

3.4 Results on Monomials

Next, we shall consider Conjecture 2.

Lemma 3.6 *For any $1 < s < k$ we have*

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

Proof. There are two cases to be considered.

Case 1: $\gcd(s, k-1) = 1$

Fermat's theorem asserts that

$$s^{\varphi(k-1)} \equiv 1 \pmod{k-1}$$

where φ is the Euler's function, which implies

$$x^{s^{\varphi(k-1)}} y^{k-s^{\varphi(k-1)}} = xy^{k-1}.$$

It is easy to see that $x^{s^{\varphi(k-1)}} y^{k-s^{\varphi(k-1)}}$ can be obtained from $x^s y^{k-s}$ by repeated application of functional composition. So the assertion of the lemma follows.

Now put $t = k - s$ for $1 < s < k$.

The case $\gcd(t, k-1) = 1$ is handled similarly.

Case 2: $\gcd(s, k-1) \neq 1$ and $\gcd(t, k-1) \neq 1$

In this case we prove the following claim.

Claim. For some $c > 1$, $s^c + t^c - (st)^c \equiv 1 \pmod{k-1}$

Proof of Claim. Since k is a prime, $\gcd(s,t) = 1$. Let $k - 1 = \alpha \cdot \beta \cdot \gamma$ such that $\gcd(s, \beta\gamma) = 1$ and $\gcd(t, \alpha\gamma) = 1$. Then, again, by Fermat's theorem we have

$s^{\varphi(\beta\gamma)} \equiv 1 \pmod{\beta\gamma}$ and $t^{\varphi(\alpha\gamma)} \equiv 1 \pmod{\alpha\gamma}$.

Let $c = \varphi(\alpha\gamma) \cdot \varphi(\beta\gamma)$ then $c > 1$ and c satisfies

$$s^c \equiv 1 \pmod{\beta\gamma} \quad \text{and} \quad t^c \equiv 1 \pmod{\alpha\gamma}.$$

This means that there exists $m, n \in \mathbf{N}$ such that

$$s^c = 1 + m(\beta\gamma) \quad \text{and} \quad t^c = 1 + n(\alpha\gamma),$$

from which it follows that

$$(s^c - 1)(t^c - 1) = (\alpha\beta\gamma)(mn\gamma).$$

Hence we have

$$s^c + t^c - (st)^c \equiv 1 \pmod{k-1}$$

for some $c > 1$. This completes the proof of Claim.

As in Case 1, it is not difficult to see that $x^u y^{k-u}$ for $u = s^c + t^c - (st)^c$ can be obtained from $x^s y^{k-s}$ by repeated application of functional composition. Therefore the assertion of the lemma holds. □

On the other hand, it is readily verified that $x^s y^{k-s}$ where $1 < s < k$ cannot be obtained from xy^{k-1}. Hence we have:

Corollary 3.7 *Let k be a prime and $1 < s < k$. Then $x^s y^{k-s}$ is not minimal.*

To conclude, Conjecture 2 is settled affirmatively by Proposition 3.4 and Corollary 3.7.

Theorem 3.8 *Let k be a prime and $1 < s < k$. Then xy^{k-1} is a unique monomial which is minimal (up to the interchange of variables).*

References

[Cs83] Csákány, B. (1983). All minimal clones on the three-element set, *Acta Cybernet.*, **6**, 227-238.

[IM59] Ianov, Iu. I. and Mutchnik, A.A. (1959). Existence of k-valued closed classes without a finite basis (in Russian), *Dokl. Akad. Nauk.*, **127**, 44-46.

[MP06] Machida, H. and Pinsker, M. (2006). Some observations on minimal clones, to appear in *Proceedings 36th International Symposium on Multiple-Valued Logic*, IEEE.

[PK79] Pöschel, R. and Kaluzhnin, L. A. (1979). *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften, 259pp.

[Po41] Post, E.L. (1941). The two-valued iterative systems of mathematical logic, *Ann. Math. Studies*, **5**, Princeton Univ. Press.

[Ro70] Rosenberg, I.G. (1970). On the functional completeness in many-valued logics (Über die funktionale Vollständigkeit in dem mehrwertigen Logiken, in German), *Rozpravy Československé. Akad. Věd. Řada Mat. Prírod. Věd.*, **80**, 3-93.

[Ro86] Rosenberg, I. G. (1986). Minimal clones I: The five types, *Colloq. Math. Soc. J. Bolyai*, **43**, 405-427.

[Sze86] Szendrei, Á. (1986). *Clones in Universal Algebra*, SMS Series **99**, Les Presses de L'Université de Montréal, 166pp.