Weak Generators on Finite Sets.

Abstract. For any finite set, we construct a binary commutative operation defined with the zero, the successor and the equality relation that generates via compositions any mapping on this set. Moreover, this construction can be generalized to a ternary operator defined with the order relation that enables to generate any mapping on any finite set.

Mathematics Subjects Classification : 68Q, 06E30, 94C10.

For any $n > 0$, $\mathcal{E}_n$ is the set $\{0, 1, \ldots, n-1\}$. For convenience, we will see this set as the ring $\mathbb{Z}/n\mathbb{Z}$ equiped with the usual addition and multiplication. For any $k > 0$, $\mathcal{F}_n^k$ is the set of mappings from $\mathcal{E}_n^k$ to $\mathcal{E}_n$. $\mathcal{F}_n$ is the union $\mathcal{F}_n^1 \cup \mathcal{F}_n^2 \ldots$ and $\mathcal{R}_n$ is the set of binary relations from $\mathcal{E}_n^2$ to $\{0, 1\}$. The aim of this paper is to find, for any $n > 0$, some mapping μ_n that enables to generate via compositions all mappings of $\mathcal{F}_n$. We prove the existence of a family of such mappings that are just defined with the following elementary bricks : the zero, the successor and the equality. First, we recall some basic notions about *terms* that are formal representations of mappings. Second, we prove the theorem with purely combinatorial arguments. At last, we propose a generalization to a ternary operator that enables to generate any mapping on any finite set.

Definition. (terms). For $n > 0$ and any subset F of $\mathcal{F}_n$, a *p-term* over F is : an integer i where $1 \leq i \leq p$, or a $(k+1)$-uple $[f, T_1, \ldots, T_k]$ where $k > 0$ and f is in $F \cap \mathcal{F}_n^k$ and $T_1, \ldots, T_k$ are p-terms over F. (Observe that any p-term is a $(p+1)$-term.) Given a term T and a list L of terms $U_1, \ldots, U_m$, the term $T(L)$ is obtained by replacing any $1 \leq i \leq m$ in T by U_i :

$$T(L) = \begin{cases} U_i & \text{if } T = i \text{ and } 1 \leq i \leq m \\ i & \text{if } T = i > m \\ [f, T_1(L), \ldots, T_k(L)] & \text{if } T = [f, T_1, \ldots, T_k] \end{cases}$$

(Observe that $T = T() = T(1) = T(1,2) = \ldots$). Any p-term T is a formal representation of a mapping $\overrightarrow{T}$ in $\mathcal{F}_n^p$: for any $a = (a_1, \ldots, a_p)$ in $\mathcal{E}_n^p$,

$$\overrightarrow{T}(a) = \begin{cases} a_i & \text{if } T = i \\ f(\overrightarrow{T_1}(a), \ldots, \overrightarrow{T_k}(a)) & \text{if } T = [f, T_1, \ldots, T_k] \end{cases}$$

(Observe that $\overrightarrow{T}(a_1, \ldots, a_p, \ldots, a_{p+q}) = \overrightarrow{T}(a_1, \ldots, a_p)$). We say that a mapping $f \in \mathcal{F}_n^k$ is *constructible with* F when there exists a k-term T over F such

that $\overrightarrow{T} = f$. We say that F is *complete* when any mapping in $\mathcal{F}_n$ is constructible with F. (Hence $\mathcal{F}_n$ is complete). We say that a mapping $f \in \mathcal{F}_n$ is *universal* when $\{f\}$ is complete.

Theorem 1. *For any $n > 0$, the following mapping $\mu_n : \mathcal{E}_n^2 \longrightarrow \mathcal{E}_n$ is universal :*

$$\mu_n(x,y) = \begin{cases} x+1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

The case $n = 1$ is trivial. The case $n = 2$ is well-known since μ_2 corresponds to the NOR boolean operator. Now we fix $n \geq 3$ and $\mu = \mu_n$. Let us call *μ-term* any term over $\{\mu\}$.

Lemma 2. (basical).

(1). There exists a μ-term $NULL$ such that $\overrightarrow{NULL}(x) = 0$ for any $x \in \mathcal{E}_n$.

(2). For any $i \in \mathcal{E}_n$, there exists a μ-term $TEST_i$ such that, for any $x \in \mathcal{E}_n$:

$$\overrightarrow{TEST_i}(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{else} \end{cases}$$

(3). There exist μ-terms NOT, OR, AND such that, for any $(x,y) \in \mathcal{E}_n^2$:

x	y	$\overrightarrow{NOT}(x)$	$\overrightarrow{OR}(x,y)$	$\overrightarrow{AND}(x,y)$
0	0	1	0	0
0	1	1	1	0
1	0	0	1	0
1	1	0	0	1

Proof. (1). The μ-term $NULL = [\mu, 1, [\mu, 1, 1]]$ satisfies :
$\overrightarrow{NULL}(x) = \mu(x, \mu(x,x)) = \mu(x, x+1) = 0$. (2). Let Δ_0 be the μ-term 1 and for any $k > 0$ let Δ_k be the μ-term $[\mu, \Delta_{k-1}, \Delta_{k-1}]$. By definition of μ, one has $\overrightarrow{\Delta_k}(x) = x + k$. Now, let k be the element of $\mathcal{E}_n$ such that $i + k = 0$ (take $k = 0$ if $i = 0$ and $k = n - i$ if $i > 0$). The μ-term $T = [\mu, NULL, \Delta_k]$ satisfies $\overrightarrow{T} = TEST_i$ since :

$$\begin{aligned} \overrightarrow{T}(x) &= \mu(\overrightarrow{NULL}(x), x+k) \\ &= \mu(0, x+k) = \begin{cases} 1 & \text{if } x+k = 0 \text{ that is } x = i \\ 0 & \text{if } x+k \neq 0 \text{ that is } x \neq i \end{cases} \end{aligned}$$

(3). The μ-terms $N = [\mu, NULL, 1], O = [\mu, NULL, [\mu, 1, 2]], S = [\mu, [\mu, 1, 1], 2]$ and $A = [\mu, [\mu, S, 2], S]$ satisfy :

x	y	$\overrightarrow{N}(x)$	$\overrightarrow{[\mu,1,2]}(x,y)$	$\overrightarrow{O}(x,y)$	$\overrightarrow{[\mu,1,1]}(x,y)$	$\overrightarrow{S}(x,y)$	$\overrightarrow{A}(x,y)$
0	0	1	1	0	1	0	0
0	1	1	0	1	1	2	0
1	0	0	0	1	2	0	0
1	1	0	2	0	2	0	1

and N, O, A are respectively solutions for NOT, OR, AND.■

Lemma 3. (relations). *Any mapping in $\mathcal{R}_n$ is constructible with $\{\mu\}$.*

Proof. Let f be a mapping in $\mathcal{R}_n$. We proceed by induction on the cardinal w of the set $f^{-1}(1)$. If $w = 0$, it is obvious since $\overrightarrow{NULL} = f$. If $w > 0$ then there exists f' in $\mathcal{R}_n$ and $(i, j) \in \mathcal{E}_n^2$ such that $f(i, j) = 1$, $f'(i, j) = 0$ and $f'(x, y) = f(x, y)$ for any $(x, y) \neq (i, j)$. Hence $|f'^{-1}(1)| = w - 1$. By induction hypothesis, there exists a μ-term T' such that $\overrightarrow{T'} = f'$. The μ-term $T = OR(AND(TEST_i, TEST_j(2)), T')$ satisfies $\overrightarrow{T} = f$ since from the previous Lemma (basical), for any $(x, y) \in \mathcal{E}_n^2$:

$$\overrightarrow{T}(x,y) = \overrightarrow{OR}(\overrightarrow{AND}(\overrightarrow{TEST_i}(x), \overrightarrow{TEST_j}(y)), \overrightarrow{T'}(x,y))$$

$$= \begin{cases} \overrightarrow{OR}(1,0) = 1 & \text{if } (x,y) = (i,j) \text{ (then } f'(x,y) = 0,\ f(x,y) = 1) \\ \overrightarrow{OR}(0,0) = 0 & \text{if } (x,y) \neq (i,j) \text{ and } f'(x,y) = 0 \text{ (then } f(x,y) = 0) \\ \overrightarrow{OR}(0,1) = 1 & \text{if } (x,y) \neq (i,j) \text{ and } f'(x,y) = 1 \text{ (then } f(x,y) = 1) \end{cases}$$

■

Lemma 4. (reduce). *Any mapping in $\mathcal{F}_n^2$ is constructible with $\mathcal{R}_n \cup \{\mu\}$.*

Proof. Let f be a mapping of $\mathcal{F}_n^2$ with $f : \mathcal{E}_n^2 \longrightarrow \{0, 1, \ldots, k-1\}$. We proceed by induction on k. For $k = 2$, it is obvious since $f \in \mathcal{R}_n$ and the term $T = [f, 1, 2]$ over $\mathcal{R}_n$ satisfies $\overrightarrow{T} = f$. For $k \geq 3$, define two mappings $f_0, f_1 : \mathcal{E}_n^2 \longrightarrow \{0, 1, \ldots, k-2\}$ as follow :

$$f_0(x,y) = \begin{cases} (a-1) & \text{if } f(x,y) = a \geq 1 \\ 0 & \text{if } f(x,y) = 0 \end{cases}$$

$$f_1(x,y) = \begin{cases} (a-1) & \text{if } f(x,y) = a \geq 1 \\ 1 & \text{if } f(x,y) = 0 \end{cases}$$

By hypothesis, there exist two terms T_0, T_1 over $\mathcal{R}_n \cup \{\mu\}$ such that $\overrightarrow{T_0} = f_0$ and $\overrightarrow{T_1} = f_1$. Let T be the term $[\mu, T_0, T_1]$ over $\mathcal{R}_n \cup \{\mu\}$. Hence $\overrightarrow{T} = f$ since for any $(x,y) \in \mathcal{E}_n^2$:

$$\begin{aligned} \overrightarrow{T}(x,y) &= \mu(\overrightarrow{T_0}(x,y), \overrightarrow{T_1}(x,y)) \\ &= \mu(f_0(x,y), f_1(x,y)) \\ &= \begin{cases} \mu(a-1, a-1) = a & \text{if } f(x,y) = a \geq 1 \\ \mu(0,1) = 0 & \text{if } f(x,y) = 0 \end{cases} \end{aligned}$$

■

Lemma 5. (binary). *Any mapping in $\mathcal{F}_n^2$ is constructible with $\{\mu\}$.*

Proof. Let f be a mapping in $\mathcal{F}_n^2$. From Lemma (reduce), there exists a term T over $\mathcal{R}_n \cup \{\mu\}$ such that $\overrightarrow{T} = f$. Now, from Lemma (relations), any mapping in $\mathcal{R}_n$ is constructible with $\{\mu\}$. Define a μ-term T^* by replacing any mapping r of $\mathcal{R}_n$ that appears in T with some μ-term R such that $\overrightarrow{R} = r$ as follow :

$$T^* = \begin{cases} i & \text{if } T = i \\ [\mu, T_1^*, T_2^*] & \text{if } T = [\mu, T_1, T_2] \\ R(T_1^*, T_2^*) & \text{if } T = [r, T_1, T_2],\ R \text{ is a } \mu\text{-term such that } \overrightarrow{R} = r \end{cases}$$

By induction on the term T, we obviously have $\overrightarrow{T^*} = \overrightarrow{T} = f$.■

Lemma 6. (select). *There exists a μ-term $SELECT$ such that*

$$\overrightarrow{SELECT}(x, y_0, \ldots, y_{n-1}) = y_x$$

for any $(x, y_0, \ldots, y_{n-1}) \in \mathcal{E}_n^{n+1}$.

Proof. First, we construct a μ-term IF such that for any $(x,y,z) \in \mathcal{E}_n^3$:

$$\overrightarrow{IF}(x,y,z) = \begin{cases} y & \text{if } x = 1 \\ z & \text{if } x = 0 \end{cases}$$

Consider two mappings f and g in $\mathcal{F}_n^2$ such that $f(0,x) = 0$, $f(1,x) = x$, $g(x,0) = x$, $g(0,x) = x$ for any $x \in \mathcal{E}_n$. From Lemma (binary) f, g are constructible with $\{\mu\}$. So there exist μ-terms T_* and T_+ such that $\overrightarrow{T_*} = f$ and $\overrightarrow{T_+} = g$. The μ-term $T = T_+(T_*, T_*(NOT, 3))$ is a solution for IF since it satisfies :

$$\begin{aligned}
\overrightarrow{T}(x,y,z) &= \overrightarrow{T_+}(\overrightarrow{T_*}(x,y,z), \overrightarrow{T_*}(\overrightarrow{NOT}(x,y,z), \overrightarrow{3}(x,y,z))) \\
&= \overrightarrow{T_+}(\overrightarrow{T_*}(x,y), \overrightarrow{T_*}(\overrightarrow{NOT}(x), z)) \\
&= \begin{cases} \overrightarrow{T_+}(\overrightarrow{T_*}(1,y), \overrightarrow{T_*}(0,z)) = y & \text{if } x = 1 \\ \overrightarrow{T_+}(\overrightarrow{T_*}(0,y), \overrightarrow{T_*}(1,z)) = z & \text{if } x = 0 \end{cases}
\end{aligned}$$

Let T_0 be the μ-term $(n+1)$. For $i > 0$, let T_i be the μ-term $IF(TEST_i, i+2, T_{i-1})$. By construction, the μ-term T_{n-1} is a solution for $SELECT$.■

For $n = 3$, the μ-term $SELECT$ is $IF(TEST_0, 2, IF(TEST_1, 3, 4))$ and :

$$\begin{aligned}
\overrightarrow{SELECT}(x, y_0, y_1, y_2) &= \overrightarrow{IF}(\overrightarrow{TEST_0}(x), y_0, \overrightarrow{IF}(\overrightarrow{TEST_1}(x), y_1, y_2)) \\
&= \begin{cases} y_0 & \text{if } \overrightarrow{TEST_0}(x) = 1 \text{ else} \\ y_1 & \text{if } \overrightarrow{TEST_1}(x) = 1 \text{ else } y_2 \end{cases} \\
&= \begin{cases} y_0 & \text{if } x = 0 \text{ else} \\ y_1 & \text{if } x = 1 \text{ else } y_2 \end{cases}
\end{aligned}$$

Lemma 7. (general). *Any mapping of $\mathcal{F}_n$ is constructible with $\{\mu\}$.*

Proof. Let f be a mapping of $\mathcal{F}_n^k$. The case $k = 2$ is done in Lemma (binary). For $k = 1$, there exists a mapping g in $\mathcal{F}_n^2$ such that $g(x,x) = f(x)$ for any $x \in \mathcal{E}_n$. From Lemma (binary), there exists a μ-term T such that $\overrightarrow{T} = g$. So the μ-term $D = T(1,1)$ satisfies $\overrightarrow{D} = f$. Assume $k \geq 3$. Let f be a mapping of $\mathcal{F}_n^k$. For any $i \in \mathcal{E}_n$, let f_i be the mapping of $\mathcal{F}_n^{k-1}$ obtained from f by fixing the k-th component to the value i : for any $(x_1, \ldots, x_{k-1})$ in $\mathcal{E}_n^{k-1}$ the relation $f_i(x_1, \ldots, x_{k-1}) = f(x_1, \ldots, x_{k-1}, i)$ holds. By hypothesis, there exists a μ-term T_i such that $\overrightarrow{T_i} = f_i$. Let T be the μ-term $SELECT(k, T_0, \ldots, T_{n-1})$. The μ-term T satisfies $\overrightarrow{T} = f$.■

This completes the proof of Theorem 1. With this construction, one can prove properties of mappings on finite sets via some induction on commutative ones, and moreover using the very basic single one μ. Any mapping of $\mathcal{F}_n$ is either a projection or the composition of μ on two smaller mappings. As an application, we can easily obtain the following criterion of primality.

COROLLARY 8. (primal). *An integer $n \geq 2$ is prime if and only if there exists a polynomial χ in $\mathcal{E}_n[X]$ such that :*

$$\chi(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$$

Proof. Assume n is prime. Then $(n-1)!$ is non-null and admits an inverse denoted q (Wilson gives $q = n-1$). The polynomial :$\chi(x) = q.\prod_{i=1}^{n-1}(x+i)$ satisfies $\chi(0) = 1$ and $\chi(x) = 0$ for any $x \neq 0$ since there exists $1 \leq i < n$ such that $x + i = 0$. Conversely, assume there is such a polynomial χ in $\mathcal{E}_n[X]$. The polynomial P in $\mathcal{E}_n[X, Y]$ such that : $P(x, y) = \chi(x - y).(x + 1)$ satisfies :

$$P(x, y) = \begin{cases} 1.(x+1) = x+1 & \text{if } x = y \\ 0.(x+1) = 0 & \text{if } x \neq y \end{cases}$$

Hence, μ is realized by P. From the Theorem, any mapping f in $\mathcal{F}_n$ is obtained by compositions of P and is polynomial. That implies that n is prime. Assume the converse $n = p.q$ with $p \geq q \geq 2$. For any $x \in \mathcal{E}_n$, $x(x+1)\ldots(x+p-1)$ is multiple of p and $x(x+1)\ldots(x+q-1)$ is multiple of q. Hence $x(x+1)\ldots(x+p-1)x(x+1)\ldots(x+q-1) = 0$ holds in $\mathcal{E}_n$. That is $x^{p+q} = r(x)$, where r is a polynomial of degree at most $p+q-1$. Hence, any polynomial function in $\mathcal{E}_n[X]$ has degree at most $p+q-1$. If $p > q \geq 2$, then $n-1 = qp-1 \geq 2p-1 > p+q-1$. So any polynomial function has degree at most $n-2$. There are at most n^{n-1} different such polynomial functions that is not enough to reach the n^n different mappings of $\mathcal{F}_n^1$. If $p = q > 2$, then $n-1 = qp-1 > 2p-1 = p+q-1$. The same argument holds. If $p = q = 2$, then $n = 4$. Any polynomial function on $\mathcal{E}_4$ has degree at most 3 (the relation $x^4 = x^2$ in $\mathcal{E}_4$ is a direct argument). There are at most 4^4 such polynomial functions : that is just enough to reach the possible mappings. However, the relations $2x^3 = 2x^2 = 2x$ hold in $\mathcal{E}_4$ too. Hence, some of the 4^4 possible polynomial functions are identified and there is a lack. ■

For instance, there is no polynomial in $\mathbb{Z}/99\mathbb{Z}[X]$ that is equal to the characteristic function of zero. Conversely, for $n = 3$, the self compositions of the polynomial $P(x, y) = (x+1)(x-y+1)(y-x+1)$ generate any mapping of $\mathcal{F}_3$.

At last, the set of all binary operators μ_n for every $n > 0$ can be generalized to a unique ternary operator on integers that enables to construct any mapping on any finite subset of $\mathbb{N}$. Say that a mapping is *integral* if for any $n > 0$ any mapping of $\mathcal{F}_n$ is definable with compositions of ϕ.

COROLLARY 9. (integral). *The following mapping* $\phi : \mathbb{N}^3 \longrightarrow \mathbb{N}$ *is integral :*

$$\phi(x,y,z) = \begin{cases} x+1 & \text{if } x = y \leq z \\ 0 & \text{else} \end{cases}$$

Proof. First, for any $n \in \mathbb{N}$, the constant mapping $C_n : \mathbb{N} \longrightarrow \{n\}$ is finitely definable with ϕ :

$$C_0(x) := \phi(\phi(x,x,x),x,x) = \phi(x+1,x,x) = 0$$
$$C_{(n+1)}(x) := \phi(C_n(x),C_n(x),C_n(x)) = \phi(n,n,n) = (n+1)$$

Now, for any $n > 0$, one can define with ϕ the universal mapping μ_n of the Theorem. For $n = 1$, that is done with C_0 and for $n > 1$, we have for any $(x,y) \in \mathcal{E}_n^2$: $\phi(x,y,C_{n-2}(x)) = \mu_n(x,y)$. Hence ϕ is integral. ■

Thanks to Professors Géraud Sénizergues and Yves Lafont for their precious questions and comments.

Serge Burckel

C.N.R.S., Institut de Mathématiques de Luminy U.P.R 9016, Campus de Luminy, 13288 Marseille cedex 9, France. burckel@iml.univ-mrs.fr

Département de Mathématiques, Université de la Réunion, 15 avenue René Cassin, 97715 Saint-Denis, France. burckel@.univ-reunion.fr