TEMPUS JEP-06015-93 LECTURE SERIES

held in Rome, February 1994
by
Béla I. Csákány (Szeged, Hungary)

FUNCTIONAL COMPLETENESS OF ALGEBRAS

An *algebra* $\mathbf{A}$ is a pair $(A; F)$ with A a non-empty set and F a set of finitary operations (i. e., mappings of form $f : A^k \to A,\ k \in \mathbf{N}$) on A.

The *projections* (or *trivial operations*) are the mappings $(a_1, \dots, a_k) \mapsto a_i$ (this is the i-th k-ary projection). The *constants* are the mappings $(a_1, \dots, a_k) \mapsto c$ (a fixed element of A). The *k-ary polynomials* of $(A; F)$ are those mappings of A^k into A which arise from projections and constants by finitely many applications of the operations in F (we apply them pointwise, i. e. if, e. g., $f_1, f_2 \in F$ are k-ary and $+ \in F$ is binary (=2-ary) then, for $a_i \in A, \qquad (f_1 + f_2)(a_1, \dots, a_k) = f_1(a_1, \dots, a_k) + f_2(a_1, \dots, a_k)$).

Notation: x_i is the i-th (k-ary) projection, c is the above constant. E. g., the unary (=1-ary) polynomials of a field $\mathbf{K} = (K; \{+, \cdot\})$ are of form

$$c_n x^n + \dots + c_1 x + c_0 \quad (c_i \in K),$$

and the k-ary polynomials of a vector space $\mathbf{V}$ over a field $\mathbf{K}$ are of form

$$c_1 x_1 + \dots + c_k x_k + u \quad (c_i \in K,\ u \in V).$$

Polynomials constructed from projections only (i. e. without use of constants) are called *term functions*; e. g., the unary term functions of $\mathbf{K}$ are $d_n x^n + \dots + d_1 x$ with all d_i integers, and the k-ary term functions of $\mathbf{V}$ are $c_1 x_1 + \dots + c_k x_k$.

An algebra $\mathbf{A}$ is called *functionally complete* if all the mappings of A^k into A (i. e., all possible finitary operations on A) are polynomials of $\mathbf{A}$. The algebra $\mathbf{A}$ is said to be *primal* if all possible operations on A are term functions of $\mathbf{A}$.

Examples: Finite fields $\mathbf{GF}(q)$ are functionally complete (f. c. in the sequel): any possible k-ary f on $\mathbf{GF}(q)$ is a polynomial, as the following equation shows:

$$f(x_1, \dots, x_k) = \sum_{a_1, \dots, a_k \in \mathbf{GF}(q)} f(a_1, \dots, a_k) \prod_{i=1}^{k} (1 - (x_i - a_i)^{q-1}).$$

The two-element Boolean algebra $\mathbf{B} = (B(= \{0,1\}); \{\vee, \cdot, {}^{-}\})$ ($(\mathbf{2}; \vee, \cdot, {}^{-})$ in a less fussy notation; in general, $\mathbf{n}$ denotes the set $0, \ldots, n-1$) is f. c., too. In fact, it is primal: any $f : B^k \longrightarrow B$ is a term function of $\mathbf{B}$, as for arbitrary $x_i \in B$ we have

$$f(x_1, \ldots, x_k) = \bigvee_{a_1, \cdots, a_k \in B} f(a_1, \ldots, a_k) \prod_{i=1}^{k} \tilde{x}_i,$$

where $\tilde{x}_i$ means x_i if $a_i = 1$ and $\bar{x}_i$ if $a_i = 0$ (observe that the constants are term functions of $\mathbf{B}$).

These examples are special cases of the following more general fact:

Werner–Wille Theorem: A finite algebra $\mathbf{A} = (A; F)$ is f. c. iff there are elements $0, 1 \in A$ and binary polynomials $+, \cdot$ of $\mathbf{A}$ such that $x + 0 = 0 + x = x$, $x \cdot 0 = 0, x \cdot 1 = x$ hold for any $x \in A$, and the characteristic function χ_a of each $a \in A$ is a polynomial of $\mathbf{A}$.

Proof: Necessity is obvious. If the conditions are fulfilled, every $f : A^k \longrightarrow A$ has an expansion of form

$$f(x_1, \ldots, x_k) = \sum_{a_1, \ldots, a_k \in A} f(a_1, \ldots, a_k) \prod_{i=1}^{k} \chi_{a_i}(x_i),$$

where parentheses for addition as well as multiplication should be placed rightwards: $(((\ldots)\ldots)\ldots)$; no associativity etc. are required! Hence $(A; \{+, \cdot, \{\chi_a : a \in A\}\})$ is f. c.; however, if $(A; G)$ is f. c., and every $g \in G$ is a polynomial of $(A; F)$, then $(A; F)$ is – a fortiori – f. c., concluding the proof.

If, for a given algebra we can prove that all constants are term functions (as we could in the case of $\mathbf{B}$), then, using this theorem, we can establish even the primality of that algebra. We shall prove several classical results in such a way.

Foster's Theorem: Let $(G; \cdot)$ be the extension of a finite group by an outer zero element 0, and let g be a cyclic permutation of G. Then $(G; \cdot, g)$ is primal.

Proof: Apply the Werner–Wille Theorem. Let $|G| = n$; then $x \cdot g(x) \cdot \ldots \cdot g^{n-1}(x) \equiv 0$, and $\{0, g(0), \ldots, g^{n-1}(0)\} = G$. Suppose k is such that $g^k(0) = 1$ and let c be such that $g^k(c) = 0$. Then we can define

$$x + y = g^{n-k}(g^k(x) \cdot g^k(y)), \quad x \cdot y = x \cdot y \ \ [!], \quad \chi_{g^r(0)}(x) = g^k(c \cdot (g^{n-r}(x))^{n-1})$$

and check that they meet the requirements of the Werner-Wille Theorem.

Foster Type Theorem for Semilattices: Let $(S; \wedge)$ be the extension of a finite semilattice with unit 1 and zero c by an outer zero element 0, and let g be a cyclic permutation of S with $g(1) = 0$ and $g(0) = c$. Then $(S; \wedge, g)$ is primal.

Proof: Let $|G| = n$; then $x \cdot g(x) \wedge \ldots \wedge g^{n-1}(x) \equiv 0$, and $\{0, g(0), \ldots, g^{n-1}(0)\} = G$. Define

$$x + y = g(g^{n-1}(x) \wedge g^{n-1}(y)), \quad x \cdot y = x \wedge y, \quad \chi_{g^r(0)}(x) = g^{n-1}(c \wedge (g^{n-r}(x)),$$

and apply the Werner–Wille Theorem.

If the finite semilattice is the chain $1 < \ldots < n-1$, then this theorem asserts that the algebra $(\mathbf{n}; min, \ ')$ with $x' \equiv x+1 \ \ (mod \ \ n)$ – *the n-element Post algebra* – is primal.

Consider the operation $x \circ y = min(x,y) + 1(mod \ \ n)$ on $\mathbf{n}$. Then squaring $x \circ y \quad n-1$ times (in the sense of $\circ$) we obtain $min(x,y)$, while $x \circ x \equiv x+1(mod \ \ n)$. Hence we get:

Sheffer–Webb Theorem: $(\mathbf{n}; \circ)$ is primal.

Usually, if $(A; f)$ is primal, f is called a *Sheffer operation.*

Another consequence of the Werner-Wille Theorem is the finite case of the classical

Theorem of Sierpinski: Every operation can be composed from (at most) binary operations.

In our terminology this means: if O_2 stands for the set of all (at most) binary operations on A, then $(A; O_2)$ is primal.

The operation

$$t(x.y,z) = \begin{cases} z & \text{if } x = y \\ x & \text{if } x \neq y \end{cases}$$

waas introduced (on any set) by Pixley; it is called *the ternary discriminator.*

Werner's Theorem: If the ternary discriminator is a polynomial of an algebra $\mathbf{A}$, then $\mathbf{A}$ is functionally complete.

Proof: Choose $0, 1 \in A$ arbitrarily. Put

$$x \cdot y = t(y,1,x), \quad x + y = t(x,0,y)$$

and

$$\chi_a(x) = \begin{cases} t(0,x,1) & \text{if } a = 0 \\ t(0,t(a,x,0),1) & \text{if } a \neq 0, \end{cases}$$

and apply the Werner–Wille Theorem.

If, for an operation f on A, say binary, there are $a, b, c \in A$ such that $f(a,c) \neq f(b,c)$ then we say that f *depends* upon its first variable. An operation f on A is called *essential* if f depends on at least two variables, and f is surjective (i. e., for every $d \in A$ there are $a, b \in A$ such that $d = f(a,b)$).

Let T_A denote the set of all selfmaps of A.

The Słupecki Criterion: If $2 < |A| < \infty$ then $(A; T_A, f)$ is primal, whenever f is essential.

For simplicity, we prove this for binary f only. In the proof we shall apply the following

Improved Version of the Werner–Wille Theorem: Let $\mathbf{A} = (A; F)$ be finite; $0, 1 \in B \subseteq A$. All finitary operations on A whose range is contained in B are polynomials of $\mathbf{A}$ iff there are binary polynomials $\cdot, +$ of $\mathbf{A}$ such that $x+0 = 0+x = x$, $x \cdot 0 = 0$, $x \cdot 1 = x$ if $x \in B$, and the characteristic function of each element of A is a polynomial of $\mathbf{A}$. (The above proof works without change.)

Call a subset of A^2 a *square* (more accurately: a *t-square*) if it is of form $A_1 \times A_2$ where $A_1, A_2 \subseteq A$, $|A_1| = |A_2| = t$.

Yablonski Lemma: Let $\circ$ be a binary operation on A, depending on both variables, whose range contains at least three elements. There exists a 2-square on which $\circ$ takes on at least three distinct values.

Consequences of the Yablonski Lemma: 1. In the Y. Lemma, we can write t and $t-1$ $(3 \leq t \leq |A|)$ instead of 3 and 2.

2. Under the conditions of the Y. Lemma, there exists a 2-square S and an element $c \in A$ such that $\circ$ takes on the value c on S exactly once.

Proof of the Słupecki Criterion: Suppose $\mathbf{A} = (A; T_A, \circ)$ with $2 < |A| < \infty$ and $\circ$ essential. Let $g : A_k \longrightarrow A$ have a t-element range. By induction on t, we show that g is a term function of $\mathbf{A}$. Let $0, 1, \ldots, t-1$ denote the elements of the range of g.

$t = 2$. By the second consequence of the Yablonski Lemma. we have a 2-square $\{a_0, a_1\} \times \{b_0, b_1\}$ and $c \in A$ such that $\circ$ takes on c on that 2-square exactly once: say, $a_1 \circ b_1 = c$ but $a_i \circ b_j \neq c$ if $(i, j) \neq (1, 1)$. If, for $\psi_1, \psi_2 : A \rightarrow A$, $\psi_1(i) = a_i, \psi_2(i) = b_i$ $(i = 0, 1)$, then, for $x \cdot y = \chi_c(\psi_1(x) \circ \psi_2(y))$, and $x + y = \chi_0(x) \cdot \chi_0(y))$ [De Morgan formula!] we have $0 + x = x + 0 = x$, $x \cdot 1 = x$, $x \cdot 0 = 0$ whenever $x \in (\mathbf{t} =)\{0, 1\}$, and the improved Werner-Wille-Theorem applies.

$t - 1 \rightarrow t$. By the first consequence of the Yablonski Lemma, there is a $(t-1)$-square $C \times D$ on which $\circ$ takes on all the t values of the range of g [!]. For each $i \in \mathbf{t}$, choose elements $c_i \in C, d_i \in D$ with $c_i \circ d_i = i$. Define the k-ary operations g_0, g_1 as follows: if $g(u_1, \ldots, u_k) = i$, then let $g_0(u_1, \ldots u_k) = c_i$, $g_1(u_1, \ldots, u_k) = d_i$. Now $g(u_1, \ldots, u_k) = g_0(u_1, \ldots, u_k) \circ g_1(u_1, \ldots, u_k)$, and g_0, g_1 are term functions of $\mathbf{A}$ by inductive hypothesis as their ranges consist of (at most) $t-1$ elements. Thus, g is a term function of $\mathbf{A}$, too, which was needed.

Yablonski's Improvement: Instead of T_A, the set of all non-invertible self-maps of A is sufficient. (Indeed, the unary operations used in the proof can be chosen to be non-invertible.)

Salomaa's Improvement: If $|A| > 4$ then, instead of T_A, the set of all permutations of A is sufficient. (The reasoning is similar.)

It is natural to ask whether statements analogous to the Słupecki Criterion are valid for more sophisticated mathematical structures, e. g., for topological spaces and ordered sets (instead of finite sets). A sample: if M_I stands for the set of all monotonic continuous selfmaps of I (the interval $[0, 1]$ of the real line), and f is an *arbitrary*, monotonic, continuous, *essential* operation on I, does the set of term functions of $(I; M_I, f)$ comprise all monotonic, continuous operations on I? (It is known that for I and also for other compact spaces there exists a binary operation $\circ$ – e. g., $x \circ y = min(1, x + y)$ in the case of I – such that all continuous operations on I are term functions of the algebra $(I; C_I, \circ)$, where C_I is the set of all continuous selfmaps of I. This was proved by A. A. Malcev (Jr.) on the base of results of Arnold and Kolmogorov.)

Next we give some applications of the Słupecki Criterion. First we prove that the *stone-scissors-paper algebra* is functionally complete (a result of Quackenbush). This is $(\mathbf{3}; \circ)$ with Cayley table

0	0	2
0	1	1
2	1	2

Clearly, $\circ$ is essential. As for the selfmaps of $\mathbf{3}$, it is enough to represent by polynomials

1) all transpositions, and

2) a selfmap of defect 1 (i. e., with 2-element range)

as they together generate the semigroup of all selfmaps of $\mathbf{3}$; the same is true for any finite set $\mathbf{m}$. The cycle (012) is an automorphism of $(\mathbf{3}; \circ)$, hence it suffices to represent (01) as a polynomial of $(\mathbf{3}; \circ)$. Here it is:

$$(x \circ 1 \circ 2 \circ 0) \circ (x \circ 2) \circ (x \circ 1 \circ 2 \circ 0 \circ 1).$$

(You can try to find a shorter polynomial for (01)). Finally, $x \circ 0$ is a selfmap of $\mathbf{3}$ with defect 1.

The *dual discriminator* (introduced by Pixley and Fried) is defined by

$$t(x.y, z) = \begin{cases} x & \text{if } x = y \\ z & \text{if } x \neq y. \end{cases}$$

(Cf. the ternary discriminator.) For $m \geq 3$, the algebra $(\mathbf{m}; d)$ is functionally complete. First, $d(x, x, x) \equiv x$ (i. e., d is *idempotent*), hence its range is $\mathbf{m}$. Observe

$$d(2, 1, 2) \neq d(1, 1, 2) \neq d(1, 2, 2) \neq d(1, 2, 1).$$

This shows that d depends on each variable; thus, d is essential. Note that all permutations of $\mathbf{m}$ are automorphisms of $(\mathbf{m}; d)$, hence it suffices to represent – as a polynomial – (01) only. Define the polynomials $g_k(x)$ by

$$g_1(x) = d(1, d(2, d(0, x, 2), 1), 0),$$

and

$$g_k(x) = d(k, x, g_{k-1}(x)).$$

Then $g_{m-1}(x) = (01)$, and – as a bonus – $g_{m-2}(x)$ is a selfmap of $\mathbf{m}$ with defect 1.

The *n-ary near-projections* ($n \geq 3$) (introduced by Marczewski) are defined for $1 \leq j, k \leq n,\ j \neq k$ by

$$l_j^k(x_1, \ldots, x_n) = \begin{cases} x_j & \text{if } x_1, \ldots, x_n \text{ are pairwise different,} \\ x_k & \text{otherwise.} \end{cases}$$

For arbitrary $1 \leq j, k \leq n \leq m,\ \ j \neq k$, the algebra $(\mathbf{m}; l_j^k)$ is functionally complete.

The proof is tedious, hence we restrict ourselves to the case $l = l_3^1$, where the trick is similar to that for the dual discriminator. First, l is essential; this can be established in the same way as we did it for d. Again – by the same reason – we need only polynomial representations for both (01) and a selfmap of $\mathbf{m}$ with defect 1. Define the polynomials $g_k(x)$ by

$$g_2(x) = l(l(2, x, 0), x, l(x, 2, 1))$$

and

$$g_k(x) = l(x, k, g_{k-1}(x)).$$

Then $g_{m-1}(x) = (01)$, and, for $m > 3$, $g_{m-2}(x)$ is a selfmap of $\mathbf{m}$ with defect 1 (find an appropriate g_1 for $m = 3$!)

The two discriminators and the near-projections are pattern functions in the following sense. Two n-tuples $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A^n$ are said to be of the same pattern if, for $1 \leq i < j \leq n$, $a_i = a_j$ implies $b_i = b_j$ and vice versa, or, equivalently, if there exists a permutation π of A with $b_1 = \pi(a_1), \ldots, b_n = \pi(a_n)$. After Quackenbush, we call an operation $f : A^n \to A$ a *pattern function*, if

1) $f(a_1, \ldots, a_n) \in \{a_1, \ldots, a_n\}$ for arbitrary $a_i \in A$ (operations with this property are called *quasi-projections*), and

2) if $f(a_1, \ldots, a_n) = a_i$, and $(a_1, \ldots, a_n), (b_1, \ldots, b_n)$ are of the same pattern, then $f(b_1, \ldots, b_n) = b_i$.

If a pattern function is not a projection then it is at least ternary. The set of all pattern functions is infinite on any set consisting of at least two elements.

Theorem: If $m \geq 3$ and f is a pattern function on $\mathbf{m}$ then $(\mathbf{m}; f)$ is functionally complete.

Proof: Given an arbitrary operation $g : A^n \to A$, we can obtain a new operation $g' : A^{n-1} \to A$ by *identifying two* arbitrary *variables* of g (say, the first two variables):

$$g'(a_1, a_2, \ldots, a_{n-1}) = g(a_1, a_1, \ldots, a_{n-1})$$

for any $(a_1, \ldots, a_{n-1}) \in A^{n-1}$. Now

g' is a pattern function whenever g is a pattern function, and

g' is a term function of $(A; g)$: $g' = g(x_1, x_1, x_2, \ldots, x_{n-1})$, where $x_1, \ldots, x_{n-1}$ are the first etc. $(n-1)$-ary projections.

Note that if g' is a polynomial of (A, g) and $(A; g')$ is f. c. then $(A; g)$ is f. c., too. Hence the proof will be concluded if we find a set S of operations on $\mathbf{m}$ such that

1) for any pattern function f on $\mathbf{m}$ there exists a $f_S \in S$ which can be obtained from f by successive identifications of two variables, and

2) if $h \in S$ then $(\mathbf{m}; h)$ is functionally complete.

We claim that we can choose the union of the set of all non-trivial ternary pattern functions and the set of all non-trivial near-projections on $\mathbf{m}$ for S. First we show that this S satisfies 2). We have proved that, for non-trivial near-projections h, $(\mathbf{m}; h)$ is f. c.; thus, it remains to show that $(\mathbf{m}; p)$ is f. c. for every non-trivial *ternary* pattern function p.

Here is the list of the 24 non-trivial ternary pattern functions p_i $(i = 1, \ldots, 24)$ (on *any* $\mathbf{m}$ with $m \geq 3$:

$$\begin{array}{rcccccccccccccc}
 & & p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & p_9 & p_{10} & p_{11} & p_{12} \\
p_i(x,x,y) & = & x & x & x & x & x & x & x & x & x & x & x & x \\
p_i(x,y,x) & = & x & x & x & x & x & x & y & y & y & y & y & y \\
p_i(x,y,y) & = & x & x & x & y & y & y & x & x & x & y & y & y \\
p_i(x,y,z) & = & x & y & z & x & y & z & x & y & z & x & y & z
\end{array}$$

and

$$\begin{array}{rcccccccccccccc}
 & & p_{13} & p_{14} & p_{15} & p_{16} & p_{17} & p_{18} & p_{19} & p_{20} & p_{21} & p_{22} & p_{23} & p_{24} \\
p_i(x,x,y) & = & y & y & y & y & y & y & y & y & y & y & y & y \\
p_i(x,y,x) & = & x & x & x & x & x & x & y & y & y & y & y & y \\
p_i(x,y,y) & = & x & x & x & y & y & y & x & x & x & y & y & y \\
p_i(x,y,z) & = & x & y & z & x & y & z & x & y & z & x & y & z
\end{array}$$

Observe:
$p_1 = x_1$, $p_{11} = x_2$, $p_{18} = x_3$ are the ternary projections;
$p_{13} = t$ is the ternary discriminator, and $p_7, p_8, p_{15}, p_{23}, p_{24}$ can be obtained from t by permutations of variables (we say that they are *permutable from* t), and hence they are term functions of $(\mathbf{m}; t)$;
$p_6 = d$ is the dual discriminator, and p_4, p_5 are permutable from d;
$p_3 = l_3^1$, $p_{12} = l_3^2$, $p_2 = l_2^1$, $p_{17} = l_2^3$, $p_{10} = l_1^2$, $p_{16} = l_1^3$ are the non-trivial ternary near-projections; they are permutable from each other;
$s = p_{19}, p_{20}, p_{21}$ are minority functions permutable from each other;
$e = p_{22}, p_9, p_{14}$ are permutable from each other.

We have proved the functional completeness of $(\mathbf{m}; p_i)$ for $i = 3, 6, 13$ whence the same follows for $i = 12, 2, 17, 10, 16, 4, 5, 7, 8, 15, 23, 24$. Finally,

$$s(x, s(x,y,z), z) = l_1^2(x,y,z),$$
$$e(x, e(x,y,z), z) = l_2^3(x,y,z),$$

hence $(\mathbf{m}; p_i)$ are f. c. for $i = 19, 22$, and, by the same reason as above, also for $i = 20, 21, 9, 14$. Thus, our S satisfies 2).

As for 1), consider a pattern function f with at least four variables. There are two possibilities:

a) By *appropriate* successive identifications of variables we get a sequence of operations $f = f_0, f_1, \ldots, f_k$ such that

a1) every f_i is non-trivial,

a2) each f_i $(i > 0)$ arises freom f_{i-1} by identifying two variables,

a3) f_k is a ternary non-trivial pattern function.

b) By *arbitrary* successive identifications of variables of f we reach an operation g which is at least quaternary, and the identification of any two of its variables gives a projection.

In the case a), $(\mathbf{m}; f_k)$ is f. c. (as it was proved), hence $(\mathbf{m}; f)$ is f. c., too. For the case b), we are going to prove that g is always a near-projection; hence $(\mathbf{m}; g)$ is f. c., implying that $(\mathbf{m}; f)$ is f. c., which concludes the proof.

Swierczkowski Lemma: If g is an at least quaternary operation which turns into a projection under any identification of two variables then g turns always into the same projection (i. e., there exists an i such that g turns always into the ith projection).

We prove this for quaternary g, without loss of generality. Suppose that the Lemma is false. Then, up to a permutation of variables, we have one of the following four cases, each of which leads to a contradiction (instead of $g(a, b, c, d)$, we always write $abcd$ here):

(1)
$$xxuv = u \Longrightarrow xxxv = x$$
$$xyxv = v \Longrightarrow xxxv = v$$

(2)
$$xxuv = u \Longrightarrow xxvv = v \Longrightarrow xyvv = v$$
$$xyxv = y \Longrightarrow xyxx = y \Longrightarrow xyvv = y$$

(3)
$$xxuv = x \Longrightarrow xxvv = x$$
$$xyvv = v \Longrightarrow xxvv = v$$

(4)
$$xxuv = u \Longrightarrow xxux = u \Longrightarrow xyux = u$$
$$xyvv = y \Longrightarrow xyxx = y \Longrightarrow xyux = y.$$

By this Lemma, pattern functions fulfilling its assumptions are near-projections which was needed.

Since now on, we shall use the notion of a clone. Given a set A, any set C of (finitary) operations on A (i. e., mappings of form $A^n \to A$, where n is *not* fixed) is called a *clone* if C contains all the projections and it is closed under composition of operations (i. e., together with any operations $f, g_1, \ldots, g_n \in C$, f n-ary, g_i k-ary, C contains also the k-ary operation $f(g_1, \ldots, g_n)$, defined by

$$(f(g_1, \ldots, g_n))(a_1, \ldots, a_k) = f(g_1(a_1, \ldots, a_k), \ldots, g_n(a_1, \ldots, a_k))$$

for $a_1, \ldots, a_k \in A$ – we apply f *pointwise* here).

The *trivial clones* are the set $\mathcal{O}_A$ of all operations on A, and the set $\mathcal{P}_A$ of all projections of A. Clearly, all clones on a given set A form a (complete) lattice with zero and unit elements $\mathcal{P}_A$ and $\mathcal{O}_A$, respectively. For any algebra $\mathbf{A}$, the term functions of $\mathbf{A}$ form a clone *Clo* $\mathbf{A}$, in virtue of the definition of term functions. Similarly, all polynomials of $\mathbf{A}$ form a clone, too. (Notation: *Pol* $\mathbf{A}$.) An algebra $\mathbf{A}$ is primal iff *Clo* $\mathbf{A} = \mathcal{O}_A$; it is functionally complete iff *Pol* $\mathbf{A} = \mathcal{O}_A$.

We say that a clone $\mathcal{C}$ is generated by a set F of operations (in sign: $\mathcal{C} = [F]$) if $\mathcal{C}$ is the intersection of all clones containing F, or, equivalently, if every $f \in \mathcal{C}$ can be obtained from operations in F and projections by finitely many compositions Thus, $(A; F)$ is primal means $[F] = \mathcal{O}_A$, and, similarly, $(A; F)$ is f. c. iff $[F \cup A] = \mathcal{O}_A$, where on the left side A stands for the set of all constant selfmaps of A.

Recall that there exists a Sheffer operation on any finite set A. The Zorn Lemma implies that every clone $\mathcal{C}(\neq \mathcal{O}_A)$ on A can be extended to some maximal proper subclone of $\mathcal{O}_A$ (shortly: to some *maximal clone* on A). Furthermore, $[F] = \mathcal{O}_A$ if and only if for each maximal clone M on A there exists an $f \in F$ with $f \neq M$. Hence it can be suspected that the knowledge of maximal clones is a strong tool to decide primality and functional completeness of algebras.

Next we reproduce Post's result giving a full list of maximal clones on $\mathbf{2}\,(= \{0,1\})$. Elements of $\mathcal{O}_\mathbf{2}$ are called *Boolean functions.* A Boolean function f is 0-*preserving* if $f(0,\ldots,0) = 0$ (1-*preserving* Boolean functions are defined analogously); it is *monotonic* if $f(a_1,\ldots,a_n) \leq f(b_1,\ldots,b_n)$ whenever $a_1 \leq b_1,\ldots,a_n \leq b_n$; it is *self-dual* if $f(a_1,\ldots,a_n) \neq f(b_1,\ldots,b_n)$ whenever $a_1 \neq b_1,\ldots,a_n \neq b_n$; it is *linear* if there are $c_1,\ldots,c_n,c \in \mathbf{2}$ such that $f(a_1,\ldots,a_n) = c_1a_1 + \ldots + c_na_n + c$ for any $a_i \in \mathbf{2}$ with *mod* 2 addition and multiplication. It is easy to check that these properties of Boolean functions define clones: all monotonic Boolean functions form a clone, etc.

Theorem of Post: The above five clones of Boolean functions and only they are maximal clones on $\mathbf{2}$.

Proof: Addition and multiplication are 0-preserving. If f is not 0-preserving then $f(0,\ldots,0) = 1$; suppose $f1,\ldots,1) = 1$, then we have that $f(x,\ldots,x)$ is the constant 1 function. As 0 preserves 0, we get that the 0-preserving operations together with an arbitrary operation which is not 0-preserving generate a clone $\mathcal{C}$ on $\mathbf{2}$ containing $+,\cdot,0,1$, and – as $(\mathbf{2};+,\cdot)$ is a finite field and hence functionally complete – $\mathcal{C} = \mathcal{O}_\mathbf{2}$. Now suppose $f(1,\ldots,1) = 0$; then $f(x,\ldots,x) = \chi_0(x)$, and we can apply the Werner-Wille Theorem. In both cases, the clone of all 0-preserving Boolean functions turns out to be maximal. By symmetry, the 1-preserving functions form a maximal clone, too.

The functions $max, min, 0, 1$ are monotonic. Assume f is not. Then there exist $a_1 \leq b_1,\ldots,a_n \leq b_1$ with $f(a_1,\ldots,a_n) = 1,\ \ f(b_1,\ldots,b_n) = 0$. W. l. o. g., suppose $a_1 = \ldots = a_i = 0,\ b_1 = \ldots = b_i = 1,\ a_{i+1} = b_{i+1},\ldots,a_n = b_n$. Then $f(x,\ldots,x,a_{i+1},\ldots,a_n) = \chi_0(x)$, and the Werner–Wille Theorem applies.

The pattern function d as well as $x+1$ $(\equiv \chi_0(x))$ are self-dual. Assume f is not. W. l. o. g., suppose $f(0,\ldots,0,1,\ldots,1) = f(1,\ldots,1,0,\ldots,0) = 1$. Then $f(x,\ldots,x,x+1,\ldots,x+1) \equiv 1$, and $\chi_0(1) = 0$; i. e., we have both constants. Now, $d(x,y,0) = x \cdot y$ and

$d(x+1, y+1, 0)+1 = x+y$, i. e., we also have the field operations. Thus, the clone of all self-dual Boolean functions is maximal.

Addition and constants are linear. Assume f is not. By the functional completeness of $(\mathbf{2}; +, \cdot)$, we have $f(x_1, \ldots, x_n) = x_i x_j \ldots + \ldots$; w. l. o. g., suppose $f(x_1, \ldots, x_n) = x_1 x_2 \ldots x_i + \ldots$. Now, $f(x_1, x_2, 1, \ldots, 1, 0, \ldots, 0)$ (with $n-i$ 0's) is in the clone generated by the linear functions and f; it is of form $q(x_1, x_2) = x_1 x_2 + a x_1 + b x_2 + c$ $(a, b, c \in \mathbf{2})$. We have the following eight possibilities:

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
a	=	0	0	0	0	1	1	1	1
b	=	0	0	1	1	0	0	1	1
c	=	0	1	0	1	0	1	0	1

Making use of $x+1$ (which is also linear), in each case we obtain the $x_1 x_2$, i. e., the multiplication:

(1) $q(x_1, x_2)$ (2) $q(x_1, x_2) + 1$
(3) $q(x_1 + 1, x_2)$ (4) $q(x_1 + 1, x_2) + 1$
(5) $q(x_1, x_2 + 1)$ (6) $q(x_1, x_2 + 1) + 1$
(7) $q(x_1 + 1, x_2 + 1) + 1$ (8) $q(x_1 + 1, x_2 + 1)$

Thus, again we have the field operations and we are done.

Now we prove that there are no further maximal clones on $\mathbf{2}$. Suppose there exists one, say $\mathcal{M}$. Then there is a function $f \in \mathcal{M}$, which is not 0-preserving, hence $f(x, \ldots, x) = 1$ or $f(x, \ldots, x) = x+1$. Similarly, there is a $g \in \mathcal{M}$, which is not 1-preserving, and thus $g(x, \ldots, x) = 0$ or $g(x, \ldots, x) = x+1$. We see that either $\mathcal{M}$ contains both constants or it contains $x+1$. We have shown that from any non-monotonic function and the two constants $x+1$ $(\chi_0(x))$ can be composed; as $\mathcal{M}$ contains a non-monotonic function, it follows $x+1 \in \mathcal{M}$. Moreover, $\mathcal{M}$ contains a non-self-dual function, from which, as above, using $x+1$ we get the constant 1, then 0. Now, if $p \in \mathcal{M}$ is not linear, we can follow the proof of the maximality of the clone of all linear functions in order to obtain a function of form

$$x_1 x_2 + a x_1 + b x_2 + c \ \ (a, b, c \in \mathbf{2})$$

as well as to establish that multiplication belongs to $\mathcal{M}$. We get $\max(x, y)$ as $(x+1)(y+1)+1$ (this is one of the De Morgan formulas), and the Werner–Wille Theorem applies: $\mathcal{M} = \mathcal{O}_\mathbf{2}$, a contradiction.

From this theorem, a functional completeness criterion for two-element algebras follows: $(\mathbf{2}; F)$ is functionally complete iff F contains both non-monotonic and non-linear operations (they, of course, can happen to coincide). Indeed, no constant preserves (the) other constant, and the constants are not self-dual. Thus, if the assumption holds for F, then no maximal clone on $\mathbf{2}$ contains $F \cup \{0, 1\}$, hence $[F \cup \{0, 1\}] = \mathcal{O}_\mathbf{2}$, i. e. $(\mathbf{2}; F)$ is f. c.

A bit later on, we shall show that almost all two-element algebras are functionally complete in that sense that the proportion of the monotonic as well as the linear Boolean functions tends to 0 when the number of variables grows. Hence it is not surprising if for some Boolean functions f occurring somewhere in mathematics the algebra $(\mathbf{2}; f)$ turns out to be f. c., as this is the case, e. g., for the underlying Boolean function of the popular computer game "Life", invented by J. H. Conway. Life is played (usually by a PC) on an infinite squared board. At any time t (an integer) the state of each square can be 0 or 1 (dead or alive). If the states of the squares in a solid 3×3 block at time t are

$$\begin{array}{ccc} s_8 & s_1 & s_2 \\ s_7 & s_0 & s_3 \\ s_6 & s_5 & s_4 \end{array}$$

$(s_i \in \mathbf{2})$, then the state s of the *middle* square at time $t+1$ is defined by

$$s = \begin{cases} 1, & \text{if } s_0 = 1 \text{ and } 2 \leq \sum_{i=1}^{8} s_i \leq 3, \\ 1, & \text{if } s_0 = 0 \text{ and } \sum_{i=1}^{8} s_i = 3, \\ 0 & \text{otherwise.} \end{cases}$$

The state of the middle square at $t+1$ is a Boolean function $f = f(x_0, x_1, \ldots, x_8)$ with the states of all squares of the 3×3 block at t as variables; in such a way, we have an algebra $(\mathbf{2}; f)$ which can be considered as a description of Life. This algebra is f. c.; indeed, f is neither monotonic, nor linear:

$$f(0,1,1,1,0,\ldots,0) = 1 > 0 = f(0,1,1,1,1,0,\ldots,0);$$

and if $f(x_0, x_1, \ldots, x_8) = a_0x_0 + a_1x_1 + \ldots + a_8x_8 + a$ $(a_i, a \in \mathbf{2})$, then $a_0 = f(1,0,\ldots,0) = 0$, and similarly $a_1 = \ldots = a_8 = 0$, implying also $a = f(0,\ldots,0) = 0$, whence $f \equiv 0$, a contradiction.

An n-ary Boolean function is given by a table consisting of 2^n rows and $n+1$ columns, where the rows are all possible different n-tuples over $\mathbf{2}$ in lexicographic order, with the value of the considered function on the actual n-tuple at the end of each row:

$0\ldots000$	a_1
$0\ldots001$	a_2
$0\ldots010$	a_3
$\ldots\ldots.$	$\ldots$
$1\ldots101$	a_{2^n-2}
$1\ldots110$	a_{2^n-1}
$1\ldots111$	a_{2^n}

Let us denote by B_n, I_n, O_n, M_n, S_n, and L_n the number of all n-ary Boolean, 1-preserving, 0-preserving, monotonic, self-dual, and linear (Boolean) functions, respectively. Apparently, $B_n = 2^{2^n}$. Further, $I_n = O_n = B_n/2$, as, e. g. the functions in I_n are characterized by $a_{2^n} = 1$. Hence the number of n-ary non-1-preserving and non-0-preserving functions is $B_n/4$. In order to define an n-ary self-dual function, we can choose

$a_1, \ldots, a_{2^{n-1}}$ arbitrarily, and then the values in the lower half of the table are determined by the self-duality. Hence $S_n = 2^{2^{n-1}} = \sqrt{B_n}$. Linear functions $a_1x_1 + \ldots + a_nx_n + a$ are determined by the $n+1$ co-efficients, whence $L_n = 2^{n+1}$. Finally, no usable formula is known for M_n (its determining is called "Dedekind's Problem"; M_n is also the number of elements of the free distributive lattice of rank n). However, Kleitman proved that M_n asymptotically equals $2^{\binom{n}{[n/2]}}$ where $[x]$ means the integer part of x. We see that $S_n/B_n,\ L_n/B_n,\ M_n/B_n \to 0$ if $n \to \infty$.

Denote by P_n the number of the n-ary Sheffer functions on **2** (i. e., $P_n = |\{f \in B_n \mid (\mathbf{2}; f) \text{ is primal }\}|$). Post's Theorem shows that f is Sheffer iff none of the five maximal clones on **2** does contain f. The previous considerations imply that $P_n/B_n \to 1/4$ if $n \to \infty$, i. e., for sufficiently large n, about a quarter of all n-ary Boolean functions are Sheffer; they also show that almost all two-element algebras are f. c., a fact we have mentioned earlier.

Post's Theorem was generalized for arbitrary finite sets by I. G. Rosenberg in 1965. For a three-element set (say, **3**), the maximal clones were determined by Yablonski in the fifties. Their number is 18; here we give a list of them (in parentheses we indicate the number of maximal clones of the actual type), and also we relate them with the maximal clones of Post:

Operations preserving a constant. (2)

Self-dual operations (i. e., those preserving the cycle (01). (1)

Monotonic operations (i. e., those preserving the relation $0 < 1$. (1)

Linear operations (of $GF(2)$). (1)

Operations preserving a non-trivial subset. (6)

Operations preserving the cycle (012) (*or* (021)). (1)

Operations preserving a linear ordering of **3** (*or* its inverse). (3)

Linear operations (of $GF(3)$). (1)

Note that the clone of linear operations of $GF(3)$ does not depend upon the choice of the zero and unity in **3** because the permutations of **3** are linear (under any choice of the zero and unity).

There are further maximal clones on **3** which do not correspond to maximal clones of Post, namely:

Operations preserving a non-trivial partition of **3**. (3)

Operations preserving a non-trivial tolerance ρ on **3** with non-empty center (a *tolerance* on M is a reflexive and symmetric relation; the *center* of ρ is the set $\{c \in M | (\forall x \in M)\ c\rho x\ \}$. (3)

Operations which are non-essential (their clone is called the *Słupecki clone*). (1)

Analogously to the case of two-element algebras, a functional completeness criterion can be derived from Yablonski's result for three-element algebras: $(\mathbf{3}; F)$ is f. c. iff, for each maximal clone listed above except the subset-preserving and the cycle-preserving ones, there is an $f \in F$ which is not contained in that maximal clone. (Reason: no maximal clone of subset- or cycle-preserving operations does contain all the constants.)

Remark that this functional completeness result can be expressed in more common algebraic terms, namely: a three-element algebra is f. c. iff

it cannot be ordered, and
it is simple, and
it is tolerance-free, and
it has a non-linear operation, and
it has an essential operation.

Finally, we list all maximal clones on a finite (say, n-element) set; this is Rosenberg's mentioned result. They belong to six classes; two of them is empty when $n = 2$, and each of them is non-empty for $n > 2$.

I. Operations preserving a given bounded partial order on n (*bounded* means that there exist a least upper bound and a greatest lower bound of $\mathbf{n}$).

II.Operations of form $f(x_1,\ldots,x_n) = \epsilon_1(x_1)+\ldots+\epsilon_n(x_n)+c$, where $+$ is an elementary p-group operation on $\mathbf{n}$ (and thus case III occurs only if $n = p^k$ for some prime p), $c \in \mathbf{n}$, and ϵ_i $(i = 1,\ldots,n)$ are endomorphisms of $(\mathbf{n};+)$.

III. Operations preserving a given permutation of $\mathbf{n}$ which is of prime order and has no invariant element.

IV.Operations preserving a given non-trivial partition of $\mathbf{n}$.

V. Operations preserving a given k-ary central, reflexive, and symmetric relation on $\mathbf{n}$ $(k = 1,2,\ldots)$. A relation ρ is *reflexive* if $(a_1,\ldots,a_k) \in \rho$ whenever at least two of $a_1,\ldots,a_k$ coincide; ρ is *symmetric* if $(a_1,\ldots,a_k) \in \rho$ implies $(a_{1'},\ldots,a_{k'}) \in \rho$ for any permutation $i \mapsto i'$ of $\{1,\ldots,k\}$; ρ is *central* if it has a non-trivial center, and $c \in \mathbf{n}$ belongs to the center of ρ if $(a_1,\ldots,a_k) \in \rho$ whenever c occurs among $a_1,\ldots,a_k$.

These relations are exactly the non-trivial subsets if $k = 1$, and they are the non-trivial central tolerances if $k = 2$.

VI. Operations preserving a given k-regular relation on $\mathbf{n}$ $(3 \leq k \leq n)$. A relation ρ is *k-regular* if there are partitions $\pi_1,\ldots,\pi_t$ $(t \geq 1)$ of $\mathbf{n}$, such that each π_i consists of k (non-empty) classes, and $\pi_1(a_1) \cap \ldots \cap \pi_t(a_t) \neq \emptyset$ for arbitrary $a_1,\ldots,a_t \in \mathbf{n}$, which determine ρ in the following way: for $b_1,\ldots,b_k \in \mathbf{n}$, $(b_1,\ldots,b_k) \in \rho$ iff, for each $i \in \{1,\ldots,t\}$, there exists at least one class of π_i which contains at least two elements from $b_1,\ldots,b_k$. Notice that for $k = n$, $t = 1$, this clone is just the Słupecki clone.

This full list of maximal clones of operations on finite sets provides an efficient tool to decide the primality of a finite algebra:

Rosenberg's Theorem: A finite algebra $(A;F)$ is primal iff none of the six classes of operations I – VI does contain F.

We mention a quite surprising corollary of this theorem (due to Rousseau), which asserts that for a finite algebra with *one* operation the classes III, IV, and the unary part of V do the whole job instead of I – VI (we formulate it in a slightly weakened form):

A finite algebra $(A;f)$ is primal iff it has

no proper subalgebras,
only trivial congruences, and

only trivial automorphisms.

(Warning: functional completeness cannot be handled by this result!)

We conclude this introduction to functional completeness by showing how to apply Rosenberg's Theorem to determine the functionally complete groups (a problem where, e. g., the Słupecki Criterion seems to be useless).

Maurer–Rhodes Theorem: A finite group is functionally complete iff it is not Abelian and it is simple.

Proof: We check that no maximal clone does contain the operations of a non-Abelian simple group and the constants.

I. A finite group cannot be partially ordered.

II. A non-Abelian group of order p^k has a non-trivial center and hence it cannot be simple.

III. Constants do not preserve permutations.

IV. Simplicity means that no non-trivial partition is preserved by multiplication.

V. $(k = 1)$. Constants do not preserve subsets.

$(k > 1)$. If c is in the center of ρ then for arbitrary $p, q, r_3, \ldots, r_k \in \mathbf{n}$

$$(p, q, r - 3, \ldots, r_k) = (c, qc^{-1}, 1, \ldots, 1) \cdot (c^{-1}p, c, r_3, \ldots, r_k) \in \rho.$$

Thus, ρ is trivial.

VI. A k-regular ρ is obviously reflexive, hence always

$$(p, q, r - 3, \ldots, r_k) = (1, 1, r_3 q^{-1}, 1, \ldots, 1) \cdot (p, q, q, r_4, \ldots, r_k) \in \rho.$$

Thus, ρ is trivial, completing the proof.

Exercise: Prove the corresponding theorem for rings: a finite ring is functionally complete iff it is not a zero ring and it is simple. (This was proved by several people, e. g., Kuznecov and Werner, independently.)

References

S. Burris–H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, New York–Heidelberg–Berlin, 1981.

S. W. Jablonski–G. P. Gawrilow–W. B. Kudrjawzew, *Boolesche Funktionen und Postsche Klassen*, Akademie-Verlag, Berlin, 1970.

R. N. McKenzie–G. F. McNulty–W. F. Taylor, *Algebras, Lattices, Varieties*, Vol. I, Wadsworth & Brooks/Cole, Monterey, CA., 1987.

I. Rosenberg, *Über die funktionale Vollständigkeit in den mehrwertigen Logiken*, Academia, Praha, 1970.

Á. Szendrei, *Clones in Universal Algebra*, L'Université de Montréal, 1986.

H. Werner, *Discriminator Algebras*, Akademie-Verlag, Berlin, 1978.

B. Csákány, Homogeneous algebras are functionally complete, *Algebra Universalis* **11**(1980), 149-158.

B. Csákány, Life is functionally complete, *Algebra Universalis* **30**(1993), 149-150.