The purpose of this note is to characterize the class of all equationally complete non-associative algebras over a finite field $\mathbb{F}$ each of which has at least one associative element $\neq 0$, along the line of Tarski's method of dealing with the analogous result for equationally complete rings in [5]. We have established that the only equationally complete non-associative algebras over $\mathbb{F}$ with a non-zero idempotent element are the $p$-algebras defined in Section 1 and the only such algebras each of which has no idempotent element $\neq 0$ but an associative element $\neq 0$ are the $p$-zero-algebras in Section 1.

1. We shall use the terminology of Kalicki-Scott in Section 1 of [3] and in this Section we give the definition of $p$-algebras and $p$-zero-algebras. First a vector space over a field $\mathbb{F}$ is a system consisting of a non-empty set $A$, one binary operation, $+$, and a unary operation $f_\lambda(x) = \lambda x$ for each $\lambda$ of $\mathbb{F}$ such that these operations satisfy commutative, associative and distributive laws. A non-associative algebra (not necessarily associative) over a field $\mathbb{F}$ is a vector space with a binary operation, $\cdot$, satisfying the two distributive laws for $\cdot$ under $+$ and

$$f_\lambda(x \cdot y) = f_\lambda(x) \cdot y = x \cdot f_\lambda(y), \ \lambda \in \mathbb{F}, \ x, y \in A.$$ 

The class of non-associative algebras over $\mathbb{F}$ is equational, that is, defined by a set of equations and we can use theorems in Section 1 of [3] and Section 1 of [5] later in Section 3.

Let $\mathbb{F}$ be a finite field of characteristic $p$. The order of $\mathbb{F}$ is $p^m$ for a positive integer $m$ and the multiplicative group is a cyclic group $\{\xi, \xi^2, \ldots, \xi^{p^m-1}\}$ of order $p^m - 1$. In the rest of the paper the field $\mathbb{F}$ will be fixed as the base field of algebras concerned.

An associative algebra $\mathfrak{A}$ over a finite field $\mathbb{F}$ is called a $p$-algebra if $p$ is the characteristic of $\mathbb{F}$ and $a^{p^m} = a$ for each element $a$ of $\mathfrak{A}$ where $p^m$ is the order of $\mathbb{F}$. We note that a $p$-algebra is algebraic over its base field and has no nilpotent element $\neq 0$. It follows (Jacobson [1], p. 218)

---

1) Partially supported by NSF through its RPCT at the University of Oklahoma, summer of 1967.
that a $p$-algebra is commutative. An associative algebra $\mathfrak{A}$ over a finite field $\Phi$ of characteristic $p$ is called a $p$-zero-algebra if $a \cdot b = 0$ for all elements $a$ and $b$. The class of all $p$-algebras and that of all $p$-zero-algebras are both equational. A system of equations defining the first class is obtained from the system of equations for non-associative algebras by adding the associative law for $\cdot$ and the following two equations

$$ px + y = y, \quad x^{p^n} = x. $$

If the last equation is replaced by

$$ x \cdot y + z = z, $$

we have a system of equations defining the class of $p$-zero-algebras.

2. We shall show that every $p$-algebra is isomorphic to a subalgebra of a direct power of $\Phi$ regarded as the algebra over $\Phi$ itself. For this we use the following theorem due to McCoy and Montgomery [4]:

**Lemma 1.** An associative algebra $\mathfrak{A}$ over a field $E$ is isomorphic to a subalgebra of a direct power of associative algebras $\mathfrak{B}$ over $E$ if and only if for any given non-zero element $a$ of $\mathfrak{A}$ there exists a homomorphism $h$ of $\mathfrak{A}$ into $\mathfrak{B}$ such that $h(a) \neq 0$.

**Lemma 2.** Let $\mathfrak{A}$ be a $p$-algebra over the finite field $\Phi$ with a unit element 1 and let $a$ be a non-zero element in $\mathfrak{A}$. Then there exists a homomorphism $h$ of $\mathfrak{A}$ into the algebra $\Phi$ over $\Phi$ itself such that $h(a) \neq 0$.

**Proof.** First we shall show that the identical mapping in $\Phi$ can be extended to a homomorphism $h$ of the subalgebra $\Phi[a]$ generated by $a$ to the algebra $\Phi$. Let $\mu(x)$ be the minimum polynomial of $a$. $a$ is a root of $x^{p^n} - x$ which has a factorization over $\Phi$:

$$ x^{p^n} - x = x(x - \xi)(x - \xi^2) \ldots (x - \xi^{p^n - 1}) $$

where $\xi$ is a generator of the multiplicative group of $\Phi$. Since $\mu(x)$ is a factor of $x^{p^n} - x$, $\mu(x) = (x - \eta_1)(x - \eta_2) \ldots (x - \eta_k)$ where the $\eta_i$ are 0 or powers of $\xi$. Take one of them, say $\eta = \eta_i$, which is not 0. The identical isomorphism of the subfield $\Phi_1$ of the commutative algebra $\mathfrak{A}$ onto the algebra $\Phi$ can be extended to a homomorphism $h$ of $\Phi[a]$ to $\Phi$ such that $h(a) = \eta$. This extension is possible because the image of the minimum polynomial $\mu(x)$ of $a$ under the isomorphism has $\eta$ as its root (see, for instance, Jacobson [2], p. 6). It then remains to extend $h$ to the whole algebra $\mathfrak{A}$. Take a basis $\{e_i\}$ for $\mathfrak{A}$ which contains $a$. The desired extension is obtained by transfinite induction if the set $\{e_i\}$ is well ordered.

Now we prove the following

**Theorem 1.** Every $p$-algebra over a finite field $\Phi$ is isomorphic to a subalgebra of a direct power of algebras $\Phi$. 
Proof. If the given $p$-algebra $\mathfrak{A}$ has no unit element, we can always imbed $\mathfrak{A}$ isomorphically into a $p$-algebra $\mathfrak{A}'$ having a unit element. $\mathfrak{A}'$ is obtained from $\mathfrak{A}$ by adjoining a unit 1 in a usual way, that is, by taking a direct sum $\mathfrak{A} \oplus \mathfrak{F}1$ with obvious multiplication. It follows from Lemma 2 and 1 that $\mathfrak{A}'$ is isomorphic to a subalgebra of a direct power of algebras $\mathfrak{F}$. Hence $\mathfrak{A}$ is isomorphic to a subalgebra of a direct power of $\mathfrak{F}$.

3. We shall prove a theorem analogous to Kalicki-Scott's results for rings.

Theorem 2. Every $p$-algebra and $p$-zero-algebra are both equationally complete.

Proof. First we prove the theorem for $p$-algebras. We know that the algebra $\mathfrak{F}$ is a $p$-algebra over the field $\mathfrak{F}$ and the class of all $p$-algebras is equational. Let $\mathfrak{A}$ be any $p$-algebra. By Theorem 1 $\mathfrak{A}$ is isomorphic to a subalgebra of a direct power of $\mathfrak{F}$. Hence $\mathfrak{A}$ belongs to the class of algebras generated by the algebras $\mathfrak{F}$, which is the class of all homomorphic images of subalgebras of direct powers of $\mathfrak{F}$. We note that every $p$-algebra has at least one idempotent $\neq 0$, for instance, take $a^{p^n-1}$ of a non-zero element $a$. $\mathfrak{A}$ has a subalgebra generated by one of its idempotent elements $\neq 0$ which is isomorphic to $\mathfrak{F}$, and $\mathfrak{F}$ belongs to the class of algebras generated by $\mathfrak{A}$. It follows from Theorem 1.2, [5] that $\mathfrak{A}$ and $\mathfrak{F}$ are equationally equivalent, that is, they have the same set of identities. Consequently, any two $p$-algebras are equationally equivalent and this implies, by Theorem 1.3, [5], that every $p$-algebra is equationally complete. Next we define a $p$-zero-algebra $\mathfrak{A}_0$ to be an algebra $\mathfrak{F}u$ over $\mathfrak{F}$ where $u$ is a symbol satisfying $uu = 0$, the zero of the algebra. Then, in a similar way, we can prove the remaining case of $p$-zero-algebras if we use the following fact instead of Theorem 1: Every $p$-zero-algebra $\mathfrak{A}$ is isomorphic to a direct power of $\mathfrak{F}_0$. This follows immediately from the facts that members of any basis $\{e_v\}$ for the given $p$-zero-algebra satisfy the relations: $e_v^2 = 0$ and $e_v e_{v'} = 0$ for all indices $v$ and $v'$, and $\mathfrak{F}e_v$ is isomorphic to $\mathfrak{F}_0$.

From now on we consider non-associative algebras over the finite field $\mathfrak{F}$. Theorem 2 furnishes the proof of the sufficiency in the following two theorems.

Theorem 3. A non-associative algebra $\mathfrak{A}$ over a finite field $\mathfrak{F}$ of characteristic $p$ which has a non-zero idempotent element is equationally complete if and only if $\mathfrak{A}$ is a $p$-algebra.

Proof. We assume that $\mathfrak{A}$ is equationally complete and let $a$ be an idempotent $\neq 0$ in $\mathfrak{A}$. The subalgebra generated by $a$ is isomorphic to the algebra $\mathfrak{F}$ so that the class of algebras generated by $\mathfrak{A}$ contains $\mathfrak{F}$. It follows from Theorem 1.6, [3] that $\mathfrak{A}$ and $\mathfrak{F}$ have the same set of identities. Hence $\mathfrak{A}$ is a $p$-algebra.

Theorem 4. Let $\mathfrak{A}$ be a non-associative algebra over a finite field $\mathfrak{F}$
of characteristic \( p \) which has no idempotent \( \neq 0 \) but an associative element \( \neq 0 \). \( \mathfrak{A} \) is equationally complete if and only if \( \mathfrak{A} \) is a \( p \)-zero-algebra.

Proof. To prove the necessity we first show that \( \mathfrak{A} \) has a subalgebra homomorphic to the \( p \)-zero-algebra \( \mathfrak{A}_0 \) over \( \Phi \) in a similar way as in [5]. Let \( a \) be a non-zero associative element in \( \mathfrak{A} \) and let \( \mathfrak{B} \) be the subalgebra generated by \( a \). The principal ideal \( (a^2) \) in \( \mathfrak{B} \) does not contain \( a \). For suppose that \( a \) is in \( (a^2) \). Since \( \mathfrak{B} \) is commutative and associative, we would have, for some element \( b \) in \( \mathfrak{B} \) and some integer \( n \), \( a = b \cdot a^2 + na^2 = (b \cdot a + na)a \). This implies that \( (b \cdot a + na)^2 = b \cdot a + na \neq 0 \) which is impossible. Hence the difference algebra \( \mathfrak{B}/(a^2) \) is generated by \( a = (a^2) \) so that \( \mathfrak{B}/(a^2) \) is isomorphic to \( \mathfrak{A}_0 \) because \( a^2 = 0 \) and \( pa = 0 \). It follows then that the subalgebra \( \mathfrak{B} \) of \( \mathfrak{A} \) is homomorphic to \( \mathfrak{A}_0 \). The rest of the proof is entirely analogous to that of Theorem 3.

East Tennessee State University,
Johnson City, Tenn., U.S.A.

BIBLIOGRAPHY

   18, 39–46 (1956).