13. TAME ALGEBRAS AND E-MINIMAL ALGEBRAS

We defined a finite algebra to be tame just in case its congruence quotient \((0,1)\) is tame. For a tame algebra \(A\), we write \(M(A)\) in place of \(M_0(0_A,1_A)\); and we call the members of \(M(A)\) the minimal sets of \(A\). The minimal sets of a tame algebra \(A\) are the same as the \((0_A,1_A)\)-traces in \(A\). The statements in Theorem 2.8 have a simpler form and meaning when \((\alpha, \beta) = (0_A,1_A)\); the reader should review that theorem now and consider its meaning for tame algebras.

The shape of the congruence lattice of a finite algebra can determine that the algebra is tame. For example, the class of tame algebras includes all finite simple algebras. Any tame algebra that is not simple is Abelian. (These remarks are justified by Theorem 2.11, Examples 1.11–1.13, and Theorem 5.7.) Tame algebras are of five types. The type of a tame algebra \(A\), written \(\text{typ}(A)\), is equal to \(\text{typ}(0_A,1_A)\). In this chapter, we obtain special representations for tame algebras of types 1 and 2; we look at an ordering property of tame algebras of types 4 and 5; and we demonstrate a representation over finite fields for the E-minimal algebras of type 2 which we studied at length in the last half of Chapter 4.

**LEMMA 13.1.** Let \(A\) be a tame Abelian algebra; let \(N\) be a minimal set of \(A\) and let \(0 \in N\); define \(F'\) to be the set of all \(f \in \text{Pol}_1 A\) with \(f(A) \subseteq N\) and \(f(0) = 0\); and define \(F\) as the set of all \(f \in \text{Pol}_1 A\) with \(f(A) = N\).

1. If \(\text{typ}(A) = 1\) and \(\kappa = |\text{Clo}_1 A|\) then \(|F| \leq \kappa, |A| \leq |N|^\kappa\), and if \(A\) is simple then \(|N| \leq \max(\kappa, 2)\).

2. If \(\text{typ}(A) = 2\) and \(\kappa = |\text{Clo}_2 A|\) then \(|F'| \leq \kappa, |A| \leq |N|^\kappa\), and if \(A\) is simple then \(|N| \leq \kappa\).

**Proof.** Choose \(e \in F\) such that \(e = e^2\) (Theorem 2.8(2)). We suppose first that \(\text{typ}(A) = 1\). For any \(f \in F\) there exists \(g \in \text{Clo}_{n+1} A\) (for some \(n\)) and \(\langle a_1, \ldots, a_n \rangle = \bar{a} \in A^n\) such that \(f(x) = g(x, \bar{a})\). By Exercise 5.11(2) (or Claim 3 in the proof of Theorem 5.6), the polynomial \(eg(x, y_1, \ldots, y_n)\) depends on at most one variable. It certainly depends on \(x\); thus \(eg(x, y_1, \ldots, y_n) = eg(x, x, \ldots, x)\). Therefore we have \(h \in \text{Clo}_0 A\) such that \(f(x) = eh(x)\). From this it follows that \(|F| \leq |\text{Clo}_1 A|\). By 2.8(4), for any \(x \neq y \in A\) there is \(f \in F\) with \(f(x) \neq f(y)\). Thus \(x \mapsto (f(x) : f \in F)\) is an embedding of \(A\) into \(N^F\); so we have \(|A| \leq |N|^{|F|}\).

Finally, suppose that \(A\) is simple. Let \(\Pi = (\text{Pol}_1 A|_N) \cap (\text{Sym} \hspace{1pt} N)\). Every unary polynomial of \(A|_N\) is constant or belongs to \(\Pi\) (as \(A|_N\) is a minimal algebra). There-
fore \( \text{Con } A|_N = \text{Con}(N, I) \). Now \( A|_N \) is simple, since restriction maps \( \text{Con } A \) onto \( \text{Con } A|_N \). In order that \( (N, I) \) be simple, if \( |N| > 2 \) then \( I \) must be transitive on \( N \). Since \( |I| \leq |F| \), we get the last inequality in statement (1).

Now suppose that \( \text{typ}(A) = 2 \). Then \( A|_N \) is polynomially equivalent to a vector space \( \langle N, x + y, 0, \lambda x (\lambda \in \mathbb{K}) \rangle \) over a finite field \( \mathbb{K} \). Let \( |F'| = m \) and \( F' = \{ f_0, \ldots, f_{m-1} \} \) where for each \( i < m \), \( f_i(x) \) is of the form \( e_{g_i}(x, \bar{a}) \) with \( g_i \in \text{Clo}_{\ell+1} \) \( A \) and \( \bar{a} \in A^\ell \) (where \( \ell = |A| \)). Let \( g_i(x, y) = g_i(x, y, \ldots, y) \), choose \( a \in A \), and set \( f'_i(x) = e_{g'_i}(x, a) - e_{g'_i}(0, a) \). Then we claim that \( F' = \{ f'_0, \ldots, f'_{m-1} \} \). It is clear that \( f'_i \in F' \). If \( f'_i = f'_j \) then the function \( f'_i(x) - f'_j(x) \) is constant. Using that \( A \) is Abelian, we derive that \( f_i(x) - f_j(x) = f_i(y) - f_j(y) \) for all \( x, y \), which implies that \( f_i = f_j \) since \( f_i(0) = f_j(0) = 0 \). Thus we have \( m \) distinct functions \( f'_i \), and it follows that \( m = |F'| \leq |\text{Clo}_2 A| \).

Now using 2.8 (4) and the fact that \( \text{Pol}_1(A|_N) \cap (\text{Sym } N) \) is transitive on \( N \) in this case, we can easily see that \( F' \) separates points of \( A \), and so \( |A| \leq |N| |F'| \). Finally, suppose that \( A \) is simple. Then our vector space is simple, and of dimension 1, and it follows that \( |N| = |\mathbb{K}| = |F'| |N| \leq |F'| \). \( \square \)

This lemma just proved will be useful in the next chapter, and it introduces us to the idea of representing a tame algebra as a set of functions into a minimal set.

**Definition 13.2.** Let \( A \) be an algebra and \( k \) be a positive integer. We define an algebra, the \([k] \)-th matrix power of \( A \), which we shall denote by \( A^{[k]} \). The universe of this algebra will be the direct power set \( A^k \). For any \( n \geq 0 \) and \( f_0, \ldots, f_{k-1} \in \text{Clo}_{nk} A \) we define an \( n \)-ary operation \( [f_0, \ldots, f_{k-1}] = f \) on \( A^k \) by the rule:

\[
f(x^0, \ldots, x^{n-1}) = (f_0(x^0, \ldots, x^{n-1}), \ldots, f_{k-1}(x^0, \ldots, x^{n-1}))
\]

Here \( x^i = (x^0_i, \ldots, x^{n-1}_i) \in A^k \) and

\[
x^0 \ldots x^{n-1} = (x^0_0, \ldots, x^{n-1}_{k-1}, \ldots, x^0_{k-1}, \ldots, x^{n-1}_k) \in A^{nk}.
\]

\( A^{[k]} \) is the non-indexed algebra \( \langle A^k, F \rangle \) where \( F \) is the set of all operations of the form \( [f_0, \ldots, f_{k-1}] \) with \( \{ f_0, \ldots, f_{k-1} \} \subseteq \text{Clo}_{nk} A \) for some \( n \geq 0 \). (Note that \( F \) is a clone.)

For the purpose of formulating the next two theorems, we introduce some more concepts. An algebra \( A = \langle A, \ldots \rangle \) will be called a **reduct** of \( B = \langle B, \ldots \rangle \) iff \( A = B \) and \( \text{Clo } A \subseteq \text{Clo } B \). The algebra \( A \) will be called a **subreduct** of \( B \) iff it is a subalgebra of some reduct of \( B \). Algebras \( A \) and \( B \) are said to be **weakly isomorphic** iff \( A \) is isomorphic to an algebra \( B' = \langle B, \ldots \rangle \) such that \( \text{Clo } B' = \text{Clo } B \).

If \( B \) is a unary algebra (i.e., if its basic operations are unary) and if \( A \) is a subreduct of \( B^{[k]} \) for some \( k \geq 1 \), then it can easily be seen that \( A \) is strongly Abelian. We
shall now prove a converse of this fact for strongly Abelian tame algebras. In [22] it was proved that any strongly Abelian tame algebra $A = (A, f)$, having just one basic operation $f$ which is not constant, is weakly isomorphic to $(N, \sigma)^{(k)}$ for some $k$, where $N$ is a minimal set of $A$ and $\sigma$ is a permutation of $N$. A consequence was that any finite algebra whose congruence lattice is, say, $M_7$ has at least two basic operations. For strongly Abelian tame algebras in general, we have only been able to obtain the weaker result of the next theorem.

**Theorem 13.3.** Let $A$ be a tame algebra of type 1 (strongly Abelian) and let $N \in M(A)$ and $k = |\text{Cl}_{01} A|$. The algebra $A$ is isomorphic to a subreduct of $N^{(k)}$, where $N = \langle N, c(c \in N) \rangle$ has only constant operations.

**Proof.** Let $F$ be as in Lemma 13.1 and, using 13.1 (1), we choose an enumeration $f_0, \ldots, f_{k-1}$ of $F$. As in the proof of 13.1 (1), the map $\pi(x) = \langle f_0(x), \ldots, f_{k-1}(x) \rangle$ is a bijection of $A$ with a subset $E = \pi(A)$ of $N^k$. Letting $p_i$ be the projections of $N^k$ onto $N$, we have $p_i \pi = f_i$ for $i = 0, \ldots, k-1$. For each operation $g$ on the set $A$, there is a unique operation $g\pi$ on $E$ (having the same arity) such that $\pi : (A, g) \rightarrow (E, g\pi)$ is an isomorphism. Thus $\pi$ is an isomorphism of $A$ with a certain algebra $E = (E, \ldots)$.

Now we just have to show that every basic operation of $E$ is a restriction to $E$ of one of the operations of $N^{(k)}$.

Let $g$ be a basic $n$-ary operation of $A$ and $g\pi$ be the corresponding operation of $E$. For each $i < k$ consider the polynomial operation $f_i g(x_0, \ldots, x_{n-1})$ of $A$. By Exercise 5.11 (2), this operation depends on at most one variable. Thus there is $n_i < n$ and $f_i' \in \text{Pol}_i A$ such that $f_i g(x_0, \ldots, x_{n-1}) = f_i'(x_{n_i})$. If $f_i'$ is not constant, then $f_i'(A) = N$ (since $N \in M(A)$), and there is $k_i < k$ such that $f_i' = f_{k_i}$. In this case, take $h_i(x_0, \ldots, x_{n_i-1}) = x_{k_i}$, so that $h_i \in \text{Cl}_{0k} N$. We have, for $\tilde{y}^0 = \pi(x_0), \ldots, \tilde{y}^{n-1} = \pi(x_{n-1})$ in $E$,

$$p_i g\pi(\tilde{y}^0, \ldots, \tilde{y}^{n-1}) = f_i g(x_0, \ldots, x_{n-1}) = f_i'(x_{n_i}) = f_{k_i}(x_{n_i}) = p_{k_i}(\tilde{y}^{n_i}) = \tilde{y}_{k_i}^{n_i} = h_i(\tilde{y}^0 \ldots \tilde{y}^{n-1}).$$

If $f_i'$ is constant, say $c$, then we take $h_i = c, h_i \in \text{Cl}_{0k} N$.

We have now defined $h_0, \ldots, h_{k-1} \in \text{Cl}_{0k} N$, and in the notation of Definition 13.2, it is obvious that $g\pi$ is the restriction to $E$ of the operation $[h_0, \ldots, h_{k-1}]$ of $N^{(k)}$. \[\square\]

**Remark 13.4.** The definition of $A^{(k)}$ is related to the formation of rings of matrices. If $M$ is a module over a ring $R$, then $M^k$ can be given the structure of a module over the ring of $k$-by-$k$ matrices with entries from $R$, and this module has the same clone of term operations as $M^{(k)}$. Note that $A^{(k)}$ has the same clone of term operations as the algebra defined in Exercise 3.12 (4). The next theorem was discovered independently by P.P. Pálfy and by the authors.
THEOREM 13.5. Let $A$ be a tame algebra of type 2 (Abelian, not strongly Abelian) and let $N \in M(A)$ and $N = A|_N$. Then $N$ is polynomially equivalent to a vector space $V$ over a finite field $K$, and for some $k \leq |Cl_{2A}|$, $A$ is isomorphic to a subreduct $E$ of $N^{[k]}$ (where $E$ spans $V^k$ as a $K$-vector space if $A$ is simple).

PROOF. We choose $0 \in N$ and let $F'$ be defined as in Lemma 13.1. By 13.1 (2), $|F'| \leq |Cl_{2A}|$. Since $A|_N$ is a minimal algebra of type 2, we have a vector space $(N, +, -, 0, \ldots) = V$ over a finite field $K$, which is polynomially equivalent to $A|_N$. Let $I = \{f \in F' : f = f^2 \text{ and } f(A) = N\}$. By 2.8 (2), $I \neq \emptyset$. Notice that $F'$ is a vector subspace of $V^A$ (direct power of $V$).

We claim that $I$ spans $F'$ as vector space. Indeed, let $f \in F'$. There exists $\lambda \in K$ such that $f(x) = \lambda \cdot x$ when $x \in N$ (since $f|_N \in Pol_1 V$ and $f|_N(0) = 0$). If $\lambda \neq 0$ then $\frac{1}{\lambda} \cdot f \in I$. If $\lambda = 0$ then for any $e \in I$ we have $e - f \in I$. (Note that $e - f$ is defined on $A$ since $e(A) \cup f(A) \subseteq N$.) Thus in either event, $f$ is a linear combination of vectors in $I$.

Now let $e_0, \ldots, e_{k-1}$ form a maximal linearly independent subset of $I$. By the claim just proved, $e_0, \ldots, e_{k-1}$ span the space $F'$; and by 13.1 (2), $k \leq |Cl_{2A}|$. Hence using 2.8 (4) we can easily prove that $e_0, \ldots, e_{k-1}$ separate points of $A$, i.e., the map $\pi(x) = (e_0(x), \ldots, e_{k-1}(x))$ is a bijection of $A$ with a subset $E = \pi(A)$ of $N^k$. As in the last proof, $\pi : A \cong E$ for a certain algebra $E$ with basic operations $g_e$ ($g$ a basic operation of $A$). The projections $p_i$ of $N^k$ onto $N$ satisfy $e_i = p_\pi e_i$ for $i = 0, \ldots, k - 1$.

Now let $g$ be an $n$-ary basic operation of $A$, and $g_\pi$ be the corresponding operation of $E$. For $i < k$, using the Abelian property of $A$, we can prove that there are $c \in N$ and $\alpha_0, \ldots, \alpha_{n-1} \in F'$ such that

$$e_i g(x_0, \ldots, x_{n-1}) = \sum_{j=0}^{n-1} \alpha_j(x_j) + c.$$

Since $e_0, \ldots, e_{k-1}$ span $F'$, there are $\lambda_{jk} \in K$ such that

$$e_i g(x_0, \ldots, x_{n-1}) = \sum_{j<n, m<k} \lambda_{jm} e_m(x_j) + c.$$

This translates into: For $y_0, \ldots, y_{n-1} \in E$,

$$p_i g_\pi(y_0, \ldots, y_{n-1}) = \sum_{j,m} \lambda_{jm} y^j_m + c.$$

Since there is a similar equation for each basic operation $g$, and for each $i < k$, we conclude that $E$ is a subreduct of $N^{[k]}$.

Finally, suppose that $A$ is simple. Then $N$ is simple and $\dim V = 1$. Therefore $V^k$ is a $k$-dimensional vector space. If, now, $E$ spans a space $E < N^k$, then there exist
\[ \lambda_0, \ldots, \lambda_{k-1}, \text{not all 0, such that } \sum \lambda_i y_i = 0 \text{ for all } \bar{y} = \langle y_0, \ldots, y_{k-1} \rangle \in \overline{E}. \text{ (Since } \overline{E} \text{ cannot have } k \text{ linearly independent linear functionals } p_0, \ldots, p_{k-1}. \text{) But this means that } \sum \lambda_i e_i = 0 \text{ in the space } F, \text{ contradicting the choice of } e_i. \text{ Thus } E \text{ spans } V^k. \square \]

For tame algebras of types 4 and 5, we have found no representation result analogous to Theorems 13.3 and 13.5. (An analogous result can be proved for type 3; but it is essentially meaningless, since every finite algebra is isomorphic to a subreduct of a \([k]\)-th power of the two-element Boolean algebra.) Tame algebras of types 4 and 5 do, however, possess an interesting property which we shall now examine.

In Chapter 5 we introduced the notion of an \((\alpha, \beta)\) pre-order and proved (Theorem 5.26) that a tame quotient \((\alpha, \beta)\) in a finite algebra \(A\) has type 4 or 5 (assuming \(\text{typ}(\alpha, \beta) \neq 1\)) iff \(A\) admits an \((\alpha, \beta)\) pre-order. When this result is specialized to the case \((\alpha, \beta) = (0_A, 1_A)\), it states: A finite, tame, and not strongly Abelian algebra \(A\) has type 4 or 5 iff \(A\) has an admissible, connected, partial order; i.e., iff there exists a partial ordering \(\preceq\) of the set \(A\) such that all polynomials of \(A\) are monotone with respect to \(\preceq\) and the transitive-symmetric closure of \(\preceq\) is \(A \times A\). These facts can be summarized in the statement that tame algebras of types 4 and 5 are orderable, while those of types 2 and 3 are not orderable. The following theorem is an immediate consequence of Theorems 5.24 and 5.26.

**Theorem 13.6.** Let \(A\) be any finite simple algebra of type 4 or 5. There are six subalgebras \(\rho_0, \rho_1, \zeta_0, \zeta_1, \xi_0, \xi_1\) of \(A^2\) such that \(0_A \subset \rho_i \subseteq \xi_i \subseteq \zeta_i\) \((i = 0, 1)\), \(\rho_1 = \rho_0^2\), \(\zeta_1 = \zeta_0^2\), \(\xi_1 = \xi_0^2\), \(\xi_0 \cap \xi_1 = 0_A\), and

1. \(\rho_0\) and \(\rho_1\) are the minimal reflexive admissible relations on \(A\), and
   \[ \rho_0 \cup \rho_1 = 0_A \cup \bigcup \{N^2 : N \in M(A)\}; \]
2. \(\zeta_0, \xi_0\) are connected partial orderings of \(A\), and \(\zeta_0\) is the transitive closure of \(\rho_0\);
3. for every admissible partial ordering \(\mu\) of \(A\) such that \(0_A < \mu\), either \(\zeta_0 \leq \mu \leq \xi_0\) or \(\zeta_1 \leq \mu \leq \xi_1\).

If \(A, \rho_i, \zeta_i, \xi_i\) satisfy the statements of this theorem and \(N = \{u, v\}\) is one of the minimal sets of \(A\), then for one of \(i = 0, 1\) we have that \(\rho_i\) is the subalgebra of \(A^2\) generated by \(0_A \cup \{\{u, v\}\}\), \(\zeta_i\) is the transitive closure of \(\rho_i\), and \(\xi_i\) is the set of pairs \(\langle x, y \rangle \in A^2\) such that for every \(f \in \text{Pol}_1 A\), \(f(\langle x, y \rangle) = N\) implies \(f(y) = v\).

Some examples of simple algebras of type 5, the graph algebras of C. Shallon, and their orderings, are defined and studied in the exercises ending the next chapter.

Every finite simple lattice has type 4, and the lattice ordering is one of the two minimal admissible partial orderings \(\zeta_i\).

The final topic of this chapter is a representation theorem for E-minimal algebras of type 2. The E-minimal algebras were introduced and classified into five types in
Definition 2.14, Lemma 4.28, and Lemma 4.32. The most interesting of these are the E-minimal algebras of type 2. These algebras are characterized as finite, non-trivial, nilpotent algebras having a Mal'cev 3-ary polynomial, and having no non-constant idempotent unary polynomials other than the identity function. Our interest in them is heightened by Theorem 8.7.

We remark that the topic we are now discussing is nearly disjoint from the earlier topic of this chapter; an algebra is both tame and E-minimal iff it is minimal.

A **local ring** is any ring with identity in which the non-invertible elements form an ideal. It is easy to see that any finite non-trivial unitary module over a local ring is an Abelian E-minimal algebra of type 2. In Exercise 13.10 (3), the reader is asked to show that, conversely, every Abelian E-minimal algebra of type 2 is polynomially equivalent to a unitary module over a finite local ring.

**DEFINITION 13.7.** Let $GF(q)$ be a finite field of $q$ elements and let $k$ be a positive integer. An algebra $E(q, k)$ is defined as follows. The universe is the set $E(q, k) = (GF(q))^k$. The basic operations are simply all the operations $f$ on $E(q, k)$ for which (if $f$ is $n$-ary) there exist $\lambda_0, \ldots, \lambda_{n-1} \in GF(q)$ and operations $h_0, \ldots, h_{k-1}$ on $GF(q)$ (completely arbitrary except that $h_i$ is $n$-i-ary) so that for all $\bar{x}^0, \ldots, \bar{x}^{n-1} \in E(q, k)$:

$$f(\bar{x}^0, \ldots, \bar{x}^{n-1}) = (y_0, \ldots, y_{k-1}) \text{ where for } i < k,$$

$$y_i = \sum_{j<n} \lambda_j x_j^i + h_i(x_0^i, \ldots, x_{i-1}^0, \ldots, x_0^{n-1}, \ldots, x_{i-1}^{n-1}).$$

The operation $f$ defined by the formula is denoted by $[\lambda_0, \ldots, \lambda_{n-1}; h_0, \ldots, h_{k-1}]$, or by $[\bar{\lambda}; \bar{h}]$.

**Remark 13.8.** The basic operations of $E(q, k)$ constitute a polynomial clone containing all the polynomial operations of the vector space $GF(q)^k$. The congruence lattice of $E(q, k)$ is a $k + 1$-element chain; the congruences are the relations

$$\theta_i = \{(\bar{x}, \bar{y}) : x_j = y_j \text{ for all } j < i\},$$

and they satisfy $1 = \theta_0 > \theta_1 > \theta_2 > \cdots > \theta_k = 0$. It is quite easy to check that $[\theta_i, 1] = \theta_{i+1}$ for $i < k$, so $E(q, k)$ is nilpotent. It is also easy to see that every $e \in \text{Pol}_1(E(q, k))$ satisfying $e^2 = e$ must be constant or the identity, using that $e$ has the form $e = [\lambda_0; \bar{h}]$. In sum, $E(q, k)$ is an E-minimal algebra of type 2.

**THEOREM 13.9.** For any finite, non-trivial algebra $A$ the following are equivalent.

1. $A$ is E-minimal and of type 2.
2. $A$ is Mal'cev and isomorphic to a reduct of some algebra $E(q, k)$, where $k$ is the height of $\text{Con} \ A$. 


PROOF. The proof that (2) implies (1) is an easy deduction from the remarks above. The proof that (1) implies (2) occupies several pages.

Let $A$ be a finite algebra satisfying (1). Taking $\theta \in \text{Con} A$ with $\theta < 1_A$, $A$ is the body of a $(\theta,1)$-minimal set. Thus by Lemma 4.20, $A$ has a Mal'cev polynomial $d$ that is a permutation when any two of its variables are fixed. By Lemma 4.36, $A$ is nilpotent. We define $\text{ht}(A)$ to be the length of a maximal chain in $\text{Con} A$. (All maximal chains have the same length, since $\text{Con} A$ is modular.) By induction on $k = \text{ht}(A)$, we shall prove that $A$ is isomorphic to a reduct of some $E(q,k)$.

If $k = 1$, then $A$ is simple. Thus $A$ is $(0_A,1_A)$-minimal (by Lemma 4.28); i.e., it is minimal. In this case, $A$ is polynomially equivalent to a vector space of dimension one over $\text{GF}(q)$ for some $q$ (see 4.7, 4.10, 4.11); and so $A$ is isomorphic to a reduct of $E(q,1)$.

Now assume that $k > 1$, and that every finite, non-trivial algebra $B$ satisfying (1), of height $< k$, satisfies (2). Let $\delta$ be any minimal congruence of $A$. From the proof of Lemma 4.36, and the result of Exercise 3.8 (4), we have that $[1_A,\delta] = [\delta,1_A] = 0_A$; i.e., $\delta \subseteq Z(A)$. (The center of $A$, or $Z(A)$, is defined in Exercise 3.2 (5).) The algebra $A'/A\delta$ satisfies (1), and $\text{ht}(A') = k - 1$. Let $\phi' : A' \rightarrow (E(q',k-1),\ldots)$ be an isomorphism of $A'$ with a reduct of $E(q',k-1)$ (for some $q'$, by the induction assumption).

Let $T_0 = \phi'^{-1}((0,\ldots,0))$, an equivalence class of $\delta$, and put $T_0 = A|T_0$. By Lemma 4.28 and Theorem 4.31, $T_0$ is a $(0,\delta)$-trace; and so $T_0$ is polynomially equivalent to a 1-dimensional vector space over $\text{GF}(q)$ for some $q$. Passing to an algebra isomorphic to $A$, if necessary, we can assume that $T_0 = \text{GF}(q)$ and $T_0$ is polynomially equivalent to $E(q,1)$.

The next step is to set up a bijection between $A$ and $E(q',k-1) \times E(q,1)$. We may assume that $A' = \{T_0,\ldots,T_{u-1}\}$ ($u = (q')^{k-1}$) with $T_0 = \text{GF}(q) = E(q,1)$. For each $i < u$ choose an element $a_i \in T_i$, and choose $a_0 = 0$. Define a function $s'$ on $A$ by $s'(x) = a_i$ whenever $x \in T_i$. For $a \in A$, put $p'(a) = \phi'(a/\delta)$, and $p(a) = d(0,s'(a),a)$. Finally, for $a \in A$, put $\phi(a) = (p'(a),p(a))$. From the properties of $d(x,y,z)$, we easily deduce that $\phi$ is a bijection between $A$ and $E(q',k-1) \times E(q,1)$.

Replacing $A$ by an isomorphic algebra, we can now assume that

$$A = E(q',k-1) \times E(q,1) = E(q',1) \times \cdots \times E(q',1) \times E(q,1).$$

(The second equation is not strictly true, but it is a harmless identification of two sets by a bijection.) The elements of $A$ will be written either as

$$x = \langle \bar{x}, y \rangle, \quad (\bar{x} \in E(q',k-1); \ y \in E(q,1)),$$

or as

$$x = \langle x_0, \ldots, x_{k-1} \rangle, \quad (x_0, \ldots, x_{k-2} \in E(q',1); \ x_{k-1} \in E(q,1)).$$
For $x = (x_0, \ldots, x_{k-1})$ in $A$ and $0 < i < k$, we define
\[
p_i'(x) = (x_0, \ldots, x_{i-1}),
\]
\[
p_i(x) = x_i,
\]
\[
s(x) = (0, \ldots, 0, x_{k-1}),
\]
\[
\theta_i = \ker p_i'.
\]

We also put $p_0(x) = x_0$, $\theta_0 = 1_A$ and $p = p_{k-1}$. Note that $p' = p_{k-1}', s'(x) = (x_0, \ldots, x_{k-2}, 0)$ and $\delta = \ker p' = \ker s'$. We have secured the following facts.

(13.9.1) $\{\theta_i : i < k\} \subseteq \text{Con } A$, and since $\text{ht } (A) = k$,
\[
1_A = \theta_0 \succ \theta_1 \succ \cdots \succ \theta_{k-2} \succ \delta \succ 0_A.
\]

Moreover, $\delta \leq Z(A)$.

(13.9.2) $p' = p'_{k-1}$ is a homomorphism of $A$ onto a reduct of $E(q', k-1)$.

(13.9.3) Where $T_0 = s(A)$, we have that $p|_{T_0}$ is an isomorphism of $A|_{T_0}$ with an algebra polynomially equivalent to $E(q, 1)$.

This implies that $d((0, y), (0, z), (0, u)) = (0, y - z + u)$, since $E(q, 1)$ has a unique Mal'cev operation.

(13.9.4) Writing 0 for the element $(0, 0)$ in $A$, we have
\[
d(0, s'(x), x) = s(x) \text{ for all } x \in A.
\]

We begin our examination of the operations of $A$ by establishing some more facts.

(13.9.5)
(i) For any $f \in \text{Pol}_n A$ and $u \in A$, and for $\bar{x}, \bar{y}, \bar{z} \in A^n$ satisfying $(y_i, z_i) \in \delta$ for $i < n$, we have
\[
d(u, f(\bar{x}), f(d(\bar{x}, \bar{y}, \bar{z}))) = d(u, f(\bar{y}), f(\bar{z})).
\]

(Here $f(d(\bar{x}, \bar{y}, \bar{z}))$ denotes $f(d(x_0, y_0, z_0), \ldots, d(x_{n-1}, y_{n-1}, z_{n-1}))$.)

(ii) If $(y, z) \in \delta$ then
\[
d(u, y, z) = d(x, y, u)
\]
and
\[
d(y, u, d(u, y, z)) = d(d(u, y, z), u, y) = y.
\]

(iii) If $y \equiv z \equiv w \pmod{\delta}$ then
\[
d(u, y, z) = d(d(u, y, w), u, d(u, w, z)).
\]
These equations follow from the fact that $\delta \subseteq Z(A)$. For (i), observe that
\[ d(u, f(\bar{z}), f(d(\bar{z}, \bar{y}, \bar{y}))) = d(u, f(\bar{y}), f(d(\bar{y}, \bar{y}, \bar{y}))) = u. \]

Replacing the underlined occurrences of $y_0, \ldots, y_{n-1}$ by $z_0, \ldots, z_{n-1}$ gives the desired equation. For (ii), in the equation $d(u, \bar{z}, z) = d(z, \bar{z}, u)$, replace the underlined $z$'s by $y$, obtaining that $d(u, y, z) = d(x, y, u)$ (where $(y, z) \in Z(A)$). For the second equation of (ii), take $n = 1$ and $f(x) = x$ in (i), obtaining
\[ d(y, u, d(u, y, z)) = d(y, y, z) = z \]
(and $d(d(u, y, z), u, y) = d(y, u, d(u, y, z))$ since $(u, d(u, y, z)) \in \delta$). For (iii), again by (i) with $f(x) = x$, we have
\[ d(d(u, y, w), u, d(u, w, z)) = d(d(u, y, w), w, z) = d(z, w, d(w, y, u)); \quad \text{and} \]
\[ d(u, y, z) = d(u, w, d(w, y, z)). \]

Replacing all four underlined occurrences of $w$ by $y$ gives the elements $d(z, y, u)$ and $d(u, y, z)$, which are equal by (ii). Thus we can conclude that (iii) holds.

(13.9.6) For $x \in A$ we have $x = d(s(x), 0, s'(x)) = d(s'(x), 0, s(x))$.

This follows from (13.9.4) and (13.9.5)(ii). Our next goal is to prove

(13.9.7) For every $f \in \text{Pol}_nA$, there exist $g \in \text{Pol}_n(E(q', k - 1))$, and $h' : E(q', k - 1)^n \to E(q, 1)$, and $\lambda_0, \ldots, \lambda_{n-1} \in GF(q)$ so that for all $x_0 = (\bar{x}_0, y_0), \ldots, x_{n-1} = (\bar{x}_{n-1}, y_{n-1})$ in $A$,
\[ f(x_0, \ldots, x_{n-1}) = \left( g(\bar{x}_0, \ldots, \bar{x}_{n-1}), \sum \lambda_i \cdot y_i + h'(\bar{x}_0, \ldots, \bar{x}_{n-1}) \right). \]

This formula can be rewritten as

(13.9.7') $p'f(\bar{x}) = g(p'(\bar{x}))$ and $p(f(\bar{x})) = h(p(\bar{x})) + h'(p'(\bar{x}))$ for $\bar{x} \in A^n$,
where $h : E(q, 1)^n \to E(q, 1)$ is linear and $h'$ is arbitrary.
(Here $p(\bar{x})$ denotes the string $p(x_0), \ldots, p(x_{n-1})$.)

We know by (13.9.2) that $g$ exists. We have to find $h$ and $h'$, given $f \in \text{Pol}_nA$. To that end, we define
\[ h_0(\bar{x}) = d(0, f(s'(\bar{x})), f(\bar{x})), \]
\[ h_1(\bar{x}) = d(0, s'(f(\bar{x})), f(s'(\bar{x}))). \]
(13.9.8) We have that \( h_0, h_1 : A^n \to T_0 \) and

(i) \( h_0(\vec{x}) = h_0(s(\vec{x})) \),

(ii) \( h_1(\vec{x}) = h_1(s'(\vec{x})) \),

(iii) \( s(f(\vec{x})) = d(h_0(\vec{x}), 0, h_1(\vec{x})) \).

The truth of (13.9.8) will follow from (13.9.4) and (13.9.5) and the fact that \( f(\vec{x}), f(s'(\vec{x})), f(s'(f(\vec{x}))) \) are congruent modulo \( \delta \). To get (i), substitute \( 0, \vec{0}, s'(\vec{x}), \vec{z} \) for \( u, \vec{x}, \vec{y}, \vec{z} \) in (13.9.5)(i). Then we get

\[
h_0(s(\vec{x})) = d(0, f(s'(s(\vec{x}))), f(s(\vec{x}))) = d(0, f(\vec{0}), f(d(\vec{0}, s'(\vec{x}), \vec{z}))) = d(0, f(s'(\vec{x})), f(\vec{z})) = h_0(\vec{x}).
\]

For (ii),

\[
h_1(s'(\vec{x})) = d(0, s'(f(s'(\vec{x}))), f(s'(f(\vec{x})))) = d(0, s'(f(\vec{x})), f(s'(\vec{x}))) = h_1(\vec{x}).
\]

For (iii), take \( u, v, z, w \) in (13.9.5)(iii) to be \( 0, s'(f(\vec{x})), f(\vec{x}), f(s'(\vec{x})) \) and obtain

\[
s(f(\vec{x})) = d(0, s'(f(\vec{x})), f(\vec{x})) = d(h_1(\vec{x}), 0, h_0(\vec{x})) = d(h_0(\vec{x}), 0, h_1(\vec{x})).
\]

(The last equality is by (13.9.5)(ii), since we have \( (0, h_0(\vec{x})) \in \delta \).)

Now for \( \vec{z} \in T_0^n \), \( h_0(\vec{z}) \) is congruent to 0 modulo \( \delta \), so \( h_0(\vec{z}) \in T_0 \). This implies that \( h_0|_{T_0} \in \text{Pol}_n T_0 \), so by (13.9.3) there is \( h \in \text{Pol}_n(E(q, 1)) \) such that \( p(h_0(\vec{z})) = h(p(\vec{z})) \) for all \( \vec{z} \in T_0^n \). Thus we have

\[
h_0(\vec{z}) = h_0(s(\vec{z})) = (\vec{0}, p(h_0(\vec{z}))) = (\vec{0}, h(p(\vec{z}))),
\]

for all \( \vec{z} \in A^n \). Moreover, \( h \) must be linear, since \( h_0(\vec{0}) = 0 \). Similarly (13.9.8)(ii) implies that there is \( h' : E(q', k - 1)^n \to E(q, 1) \) satisfying \( h_1(\vec{z}) = (\vec{0}, h'(p'(\vec{z}))) \).

Finally (13.9.8)(iii) and the equation in (13.9.3) then imply that

\[
(\vec{0}, p(f(\vec{x}))) = s(f(\vec{x})) = d(h_0(\vec{x}), 0, h_1(\vec{x})) = (\vec{0}, h(p(\vec{x}))) + h'(p'(\vec{x})),
\]

This completes the proof of (13.9.7') and of (13.9.7).

It remains to show that \( q = q' \) and to "un-twist" our representation and show that \( A \) is isomorphic to a reduct of \( E(q, k) \). To do that, we study \( \text{Pol}_1 A \), and begin by noting that (13.9.7) implies
(13.9.9) For every \( f \in \text{Pol}_1 A \), there are \( \lambda' \in GF(q') \) and \( \lambda \in GF(q) \) such that for all \( x = (x_0, \ldots, x_{k-2}, y) \in A \) and for \( i \leq k - 2 \), we have:

\[
p_i(f(x)) - \lambda' x_i \text{ depends only on } p'_i(x) = (x_0, \ldots, x_{i-1});
\]

and \( p(f(x)) - \lambda y \) depends only on \( p'(x) = (x_0, \ldots, x_{k-2}) \).

We define \( \Sigma \) to be the set of triples

\[
(f, \lambda', \lambda) \in (\text{Pol}_1 A) \times GF(q') \times GF(q)
\]

that satisfy (13.9.9); and we define \( \sigma \) to be the set of pairs \( (\lambda', \lambda) \) such that \( (f, \lambda', \lambda) \in \Sigma \) for some \( f \). We shall show that \( \sigma \) is an isomorphism of \( GF(q') \) with \( GF(q) \). Note that for each \( f \in \text{Pol}_1 A \) there is a unique \( (\lambda', \lambda) \) with \( (f, \lambda', \lambda) \in \Sigma \).

(13.9.10) For \( i \leq k - 1 \),

\[
p_i(d(x, y, z)) - (p_i(x) - p_i(y) + p_i(z))
\]

depends only on \( p'_i(x), p'_i(y), p'_i(z) \). If \( (f, \lambda', \lambda), (g, \lambda', \gamma) \in \Sigma \),

then \( (f \circ g, \lambda' \gamma', \lambda \gamma) \in \Sigma \) and \( (h, \lambda' + \gamma', \lambda + \gamma) \in \Sigma \),

where \( h(x) = d(f(x), 0, g(x)) \).

In (13.9.10), the claimed property of \( d \) follows easily from (13.9.7) and the Mal'cev equations for \( d \); the other statement is then easily derived from (13.9.7).

(13.9.11) The domain of \( \sigma \) is \( GF(q') \).

To prove this claim, we recall that \( \theta_1 \prec 1_A \) where \( \theta_1 = \ker p'_1 = \ker p_0 \). Thus \( A \) is minimal of type 2 with respect to \( (\theta_1, 1_A) \). This implies that \( A/\theta_1 \) is polynomially equivalent to a vector space of dimension 1 over some \( GF(q'') \). The algebra \( p_0(A) \cong A/\theta_1 \) thus has precisely as many unary polynomials fixing 0 as it has elements; i.e., it has \( q' \) of them. In other words, \( f(x) = \lambda' x \) is a polynomial of \( p_0(A) \) for all \( \lambda' \in GF(q') \). This implies statement (13.9.11).

(13.9.12) The range of \( \sigma \) is \( GF(q) \).

This claim follows easily from (13.9.3). For every \( \lambda \in GF(q) \) there is \( f \in \text{Pol}_1 A \) with \( f((\bar{0}, y)) = (\bar{0}, \lambda y) \) for all \( y \). By (13.9.9) we have \( (f, \gamma', \gamma) \in \Sigma \) for some \( \gamma', \gamma \). Then

\[
pf((\bar{0}, y)) - \gamma \cdot y = \lambda \cdot y - \gamma \cdot y
\]

is constant, so \( \lambda = \gamma \).
(13.9.13) \( \sigma \) is an isomorphism of \( GF(q') \) onto \( GF(q) \).

This will follow by (13.9.10), (13.9.11), (13.9.12), if we establish that \( \sigma \) is a one-to-one function. At least, \( \sigma \) is a subring of \( GF(q') \times GF(q) \) projecting onto both factors. Thus it suffices to show that if \( (\lambda',0) \in \sigma \) then \( \lambda' = 0 \), and if \( (0,\lambda) \in \sigma \) then \( \lambda = 0 \). Suppose that \( (0,\lambda) \in \sigma \) and, say, \( (f,0,\lambda) \in \Sigma \). Then \( p_{0}f \) is constant, so \( f \) is not a permutation of \( A \). Since \( A \) is minimal relative to \( \langle 0_{A},\delta \rangle \), it follows that \( f|_{\mathbb{F}_{q}} \) is constant. This implies that \( \lambda = 0 \). Similarly, if \( (f,\lambda',0) \in \Sigma \), then \( f \) cannot be a permutation, and so \( f(1_{A}) \subseteq \theta_{1} \) (again we use the E-minimality). This implies that \( \lambda' = 0 \).

We now have that \( q' = q \) and \( A = E(q,k) \). Let \( B = \langle A, \ldots \rangle \) be the algebra satisfying \( \pi : B \cong A \) where \( \pi((\tilde{x},y)) = (\tilde{x},\sigma(y)) \). We claim that \( B \) is a reduct of \( E(q,k) \). To prove it, we examine any polynomial \( f \in \text{Pol}_{n}B \). By (13.9.7) and Definition 13.7, there are \( \lambda_{0},\lambda_{0}',\ldots,\lambda_{n-1},\lambda_{n-1}' \in GF(q) \) and \( h_{0},\ldots,h_{k-1} \) such that for any \( \tilde{x} \in B^{n} \) we have:

\[
(13.9.14) \quad \text{For all } i \leq k-2, \quad p_{i}(f(\tilde{x})) = \sum_{j} \lambda_{j}' \cdot p_{i}(x_{j}) + h_{i}(p_{i}'(\tilde{x})); \quad \text{while}
\]

\[
p(f(\tilde{x})) = \sigma^{-1}\left( \sum_{j} \lambda_{j} \cdot \sigma p(x_{j}) + h_{k-1}(p'(\tilde{x})) \right)
= \sum_{j} \sigma^{-1}(\lambda_{j}) \cdot p(x_{j}) + \sigma^{-1}h_{k-1}(p'(\tilde{x})).
\]

These formulas will imply that \( f \) is a polynomial of \( E(q,k) \), as soon as we know that \( \sigma^{-1}(\lambda_{j}) = \lambda_{j}' \). This is easily seen to be the case, by replacing all variables of \( f \) except the \( j \)th by 0. The formulas (13.9.14) imply that the resulting unary polynomial \( f_{j} \) corresponds to a unary polynomial \( h_{j} \) of \( A \) such that \( \langle h_{j},\lambda_{j}',\lambda_{j} \rangle \in \Sigma \). Thus \( \sigma(\lambda_{j}') = \lambda_{j} \). This completes our proof. \( \square \)

Exercises 13.10

1. Let \( A \) be a tame algebra of type 1. Let \( B = \langle N^{k}, \ldots \rangle \) be the reduct of \( N^{[k]} \) constructed in Theorem 13.3, which has a subalgebra isomorphic to \( A \). Prove that \( A \) and \( B \) generate the same variety.

2. This exercise refers to Theorem 13.5, but otherwise is the same as the first exercise.

3. Using the result in Exercise 3.2 (3), show that an E-minimal algebra of type 2 is Abelian if it is polynomially equivalent to a unitary module over a finite local ring.
(4) Show that an E-minimal algebra of type 2 has a Mal'cev term operation that is one-to-one in each variable when the others are held fixed. (Outline: Choose any maximal congruence $\delta$. Then $A$ is $\langle \delta, 1_A \rangle$-minimal of type 2. We are in the situation of Lemma 4.20 with $A = C = \langle \delta, 1_A \rangle$-body. Choose a term $h(x, y, z, \bar{a})$ and choose $\bar{a} \in A^n$ so that the polynomial operation $h(x, y, z, \bar{a})$ corresponds to $x - y + z$ in the vector space $A/\delta$. Then the term operation $f(x, y, z) = h(x, h(y, y, y, \ldots), z, y, \ldots, y)$ can be shown to also correspond to $x - y + z$ in $A/\delta$. Moreover $f \in \text{Clo}_2 A$. Starting with this $f$, the construction in the proof of Lemma 4.20 will produce a Mal'cev term operation having the desired property.)

(5) Let $f$ be an $n$-ary operation and $d$ be a Mal'cev operation of an algebra $A$. Suppose that $a_i$ and $b_i$ are congruent modulo the center of $A$ for $i = 0, \ldots, n - 1$. Prove that $d(f(\bar{a}), f(\bar{b}), f(\bar{c})) = f(d(\bar{a}, \bar{b}, \bar{c}))$. 