INDEPENDENCE ALGEBRAS

PETER J. CAMERON AND CSABA SZABÓ

ABSTRACT

An independence algebra is an algebra A in which the subalgebras satisfy the exchange axiom, and any map from a basis of A into A extends to an endomorphism. Independence algebras fall into two classes; the first are specified by a set X, a group G, and a G-space C. The second are much more restricted; we show that the subalgebra lattice is a projective or affine geometry, and give a complete classification of the finite algebras.

1. *Introduction*

Independence algebras were introduced by Gould [**5**] and Fountain and Lewin [**4**] as a setting for extending earlier results due to Howie, Erdos, Reynolds and Sullivan about the semigroups of mappings of a set or of linear mappings of a vector space (specifically, the structure of the semigroup generated by the non-identity idempotents).

An *independence algebra* is an algebra A (in the sense of universal algebra, that is, a set with a family of distinguished operations) satisfying the following two conditions:

1. *The subalgebras of A satisfy the exchange axiom.* That is, if $z \in \langle X \cup \{y\} \rangle$, $z \notin \langle X \rangle$, then $y \in \langle X \cup \{z\} \rangle$ (where $\langle X \rangle$ is the subalgebra generated by X).
   As is well known, the exchange axiom implies that any two minimal generating sets have the same cardinality. A minimal generating set is called a *basis* for A, and its cardinality is the *dimension* of A.
2. *Any map from a basis of A into A can be extended to an endomorphism of A.*

Note that the operations of A play no part in this definition, which refers only to subalgebras and endomorphisms. Our aim is to classify independence algebras; of course, we can only hope to determine the subalgebras and endomorphisms. Accordingly, we call two algebras A_1 and A_2 *equivalent* if there is a bijection $\theta : A_1 \to A_2$ such that

(i) both θ and θ^{-1} map subalgebras to subalgebras;
(ii) if $f_i : A_i \to A_i$ (for $i = 1, 2$) are maps satisfying $f_1\theta = \theta f_2$, then f_1 is an endomorphism of A_1 if and only if f_2 is an endomorphism of A_2. (We write endomorphisms on the right.)

Our classifications will be up to equivalence. Any algebra equivalent to an independence algebra is an independence algebra. In fact, for independence algebras, condition (i) is implied by condition (ii), since a subset is a subalgebra if and only if it is the image of an endomorphism.

Not surprisingly, we can do away with the algebra structure altogether, and

1991 *Mathematics Subject Classification* 08A05.

recognise independence algebras by their subalgebras and endomorphisms only. We specify the subalgebras by a *closure operator* $Y \mapsto \langle Y\rangle$. (This is a function from $\mathcal{P}(X)$ to $\mathcal{P}(X)$ satisfying

- $Y \subseteq \langle Y\rangle$,
- $(Y \subseteq Z) \Rightarrow (\langle Y\rangle \subseteq \langle Z\rangle)$,
- $\langle\langle Y\rangle\rangle = \langle Y\rangle$,
- if $x \in \langle Z\rangle$, then $x \in \langle Z_0\rangle$ for some finite $Z_0 \subseteq Z$,

for all $Y, Z \subseteq X$ and $x \in X$. A set Y is *independent* if $y \notin \langle Y \setminus \{y\}\rangle$ for all $y \in Y$; a *basis* is a maximal independent set.

PROPOSITION 1.1. *Let X be a set, $\langle\rangle$ a closure operator on X, and S a monoid of maps from X to X. Then $(X, \langle\rangle, S)$ arises from an independence algebra if and only if the following conditions hold:*
(i) the closure operator satisfies the exchange axiom;
(ii) any map from a basis into X extends to a member of S;
(iii) if two members of S agree on a set Y, then they agree on $\langle Y\rangle$;
(iv) for all $f \in S$, if $y \in \langle Y\rangle$, then $yf \in \langle Yf\rangle$.

Proof. The necessity of the conditions is clear; we prove their sufficiency. We define operators μ, one for each choice of elements $x_1, \ldots, x_k, y$ such that $\{x_1, \ldots, x_k\}$ is independent and $y \in \langle x_1, \ldots, x_k\rangle$, as follows. Take any $a_1, \ldots, a_k \in X$. By (ii), there exists $f \in S$ such that $x_i f = a_i$ for $i = 1, \ldots, k$; we set

$$\mu(a_1, \ldots, a_k) = yf.$$

By (iv), $yf \in \langle a_1, \ldots, a_k\rangle$; and (iii) guarantees that $\mu(a_1, \ldots, a_k)$ is well-defined, independent of the choice of f. (Note that different choices of $x_1, \ldots, x_k, y$ may give rise to the same operation μ.)

Let A consist of the set X equipped with all these operations. We show that A is the required independence algebra. For this, we show that the closure operator gives its subalgebras and that S is its endomorphism monoid. Then (i) and (ii) show that A is an independence algebra.

(a) *A map from X to X is an endomorphism of A if and only if it is in S.*

First, take $e \in S$, and let μ be the operation defined by $x_1, \ldots, x_k, y$. Choose any $a_1, \ldots, a_k \in X$. There exists $f \in S$ with $x_i f = a_i$ for $i = 1, \ldots, k$, and $yf = \mu(a_1, \ldots, a_k)$. Then

$$\mu(a_1 e, \ldots, a_k e) = \mu(x_1 fe, \ldots, x_k fe) = yfe = \mu(a_1, \ldots, a_k)e$$

(here we use the closure of S under composition). So e is an endomorphism of A.

Conversely, let e be an endomorphism of A. If $\{x_1, \ldots, x_d\}$ is a basis, then there exists $f \in S$ with $x_i f = x_i e$ for $i = 1, \ldots, d$ (by (ii)); then (iii) shows that $e = f \in S$.

(b) *A subset Y of X is a subalgebra if and only if it is closed.*

Suppose first that Y is a subalgebra, and let $y \in \langle Y\rangle$. Then there exists a minimal dependent set $\{x_1, \ldots, x_k, y\}$ with $x_1, \ldots, x_k \in Y$. So there is an operation μ of the algebra with $\mu(x_1, \ldots, x_k) = y$; thus $y \in Y$, since Y is a subalgebra. So Y is closed.

Conversely, let Y be closed. Let μ be the operation defined by the elements $x_1, \ldots, x_k, y$, and take $a_1, \ldots, a_k \in Y$. There is an endomorphism f with $x_i f = a_i$ for $i = 1, \ldots, k$ and $\mu(a_1, \ldots, a_k) = yf$. By (iv), $yf \in \langle a_1, \ldots, a_k\rangle \subseteq Y$. So Y is a subalgebra.

As suggested in the first paragraph, sets (with no operations) and F-vector spaces (with the binary operation of addition and a unary operation of multiplication by c for each $c \in F$) are independence algebras. Any subalgebra of an independence algebra is an independence algebra. There is a kind of 'quotient' operation which is also useful. Let A be an independence algebra, B a subalgebra of A. Let $A[B]$ denote the algebra A with a new nullary operation ν_b adjoined for each $b \in B$, having value b. Then $A[B]$ is an independence algebra, whose subalgebras are the subalgebras of A containing B, and whose endomorphisms are the endomorphisms of A fixing B elementwise.

Throughout the paper, except in the last section, we assume that all algebras have finite dimension. We let $\mathrm{Lat}(A)$, $\mathrm{End}(A)$ and $\mathrm{Aut}(A)$ denote the subalgebra lattice, endomorphism monoid, and automorphism group of A respectively. We write endomorphisms on the right, and algebra operations on the left (except for addition and multiplication).

We can now state our main results.

THEOREM 1.2. *The subalgebra lattice of an independence algebra is a Boolean lattice or a projective or affine geometry.*

THEOREM 1.3. *Any finite independence algebra is equivalent to one of the types described in the next two sections.*

2. *Trivial independence algebras*

We begin with a complete description of independence algebras of dimension 1. let G be a group, C a left G-space (possibly empty). Let $A = G \cup C$ (disjoint union); define a nullary operator ν_c with value c for each $c \in C$, and a unary operator λ_g on A for each $g \in G$ by the rule

$$\begin{aligned} \lambda_g(h) &= gh \quad \text{for } h \in G, \\ \lambda_g(c) &= g(c) \quad \text{for } c \in C. \end{aligned}$$

Then A is an independence algebra of dimension 1; its unique proper subalgebra is C, and writing down the endomorphisms is a simple exercise.

THEOREM 2.1. *Let A be any independence algebra of dimension* 1. *Let $G = \mathrm{Aut}(A)$ and $C = \langle \emptyset \rangle$. Then A is equivalent to the algebra obtained from the above construction.*

Proof. Any element of $A \setminus C$ is a basis for A, and the unique endomorphism mapping one such basis to another is an automorphism. So G acts regularly on $A \setminus C$, and we can identify this set with G so that G acts by right multiplication. Now, for $c \in C$, let f_c denote the unique endomorphism which maps $1 \in G$ to c. Then the composite $g \cdot f_c$ is an endomorphism mapping A to C, and so has the form $f_{g(c)}$ for some element $g(c) \in C$. It is readily checked that $c \mapsto g(c)$ $(g \in G)$ is a left action of G on C. With this representation, the endomorphisms coincide with those for the algebra $G \cup C$ previously constructed.

We note that 'a 1-dimensional independence algebra' is a remarkably concise axiomatization of 'a group acting on a set'.

The construction can be generalised as follows. Let X be a set, G a group, and C a left G-set. Let $A = (X \times G) \cup C$. Then we define nullary operators ν_c $(c \in C)$ with value c, and unary operators λ_g $(g \in G)$ by

$$\begin{aligned} \lambda_g((x,h)) &= (x, gh) \quad \text{for } x \in X,\ h \in G, \\ \lambda_g(c) &= g(c) \quad \text{for } c \in C. \end{aligned}$$

We obtain an independence algebra whose dimension is $|X|$; the subalgebras are all subsets of the form $(Y \times G) \cup C$ for $Y \subseteq X$, and so $\mathrm{Lat}(A)$ is isomorphic to the lattice $\mathcal{P}(X)$ of subsets of X.

An independence algebra A is called *trivial* if $\mathrm{Lat}(A) \cong \mathcal{P}(X)$ for some set X. Now, arguing as above, it is easy to show:

THEOREM 2.2. *Any trivial independence algebra A is equivalent to one of the form $(X \times G) \cup C$ as defined above.*

Thus the classification in this case is 'reduced' to that of groups acting on sets. For non-trivial finite independence algebras, our classification is much more precise.

3. *Examples*

We now list the known examples of non-trivial independence algebras.

EXAMPLE 3.1. A vector space V is an independence algebra. More generally, if W is a subspace of V, then $V[W]$ is an independence algebra whose subalgebra lattice is the subspace lattice of V/W.

EXAMPLE 3.2. Let V be a vector space over a field F with more than two elements. For each $c \in F$ with $c \neq 0, 1$, define a binary operator μ_c on V by the rule that $\mu_c(x, y) = x + c(y - x)$. This gives an independence algebra A whose subalgebras are the affine subspaces (cosets of vector subspaces) of V, and whose endomorphisms are the affine maps (generated by translations and linear transformations). In particular, the empty set and all singletons are subalgebras. If $|F| = 2$, this construction fails, since there are no such operators; we can use instead a ternary operator α given by $\alpha(x, y, z) = x + y + z$. We denote this algebra (in either case) by $\mathrm{Aff}(V)$.

If $v \in V$, then $\mathrm{Aff}(V)[v]$ is equivalent to the vector space V. However, new algebras can be obtained as follows. Let W be a vector subspace of V; let $\mathrm{Aff}(V)[+W]$ be the algebra obtained by adjoining unary operators τ_w for $w \in W$, where $\tau_w(x) = x + w$. Now the non-empty subalgebras are the affine subspaces of V containing a coset of W.

EXAMPLE 3.3. Let G be a sharply 2-transitive permutation group on X. Let $\{O_i : i \in I\}$ be the orbits of G on ordered triples of distinct elements of X. Define binary operations μ_i, for $i \in I$, by the rule

$$\begin{aligned} \mu_i(x, x) &= x; \\ \mu_i(x, y) &= z \quad \text{if } (x, y, z) \in O_i. \end{aligned}$$

We obtain a 2-dimensional independence algebra whose subalgebras are the empty set and the singletons, whose automorphism group is G, and whose proper endomorphisms are the constant maps.

Any finite sharply 2-transitive group is isomorphic to the group of mappings

$$\{x \mapsto xa + b : a, b \in F, a \neq 0\}$$

of a nearfield F (a structure satisfying all the field axioms except commutativity of multiplication and the right distributive law). All known infinite 2-transitive groups are of this form as well; but it is not known whether all infinite examples must come from nearfields (see Clay [**3**]). For a group of this form, the orbits O_i are parametrised by the elements of $F \setminus \{0, 1\}$, and the operations μ_i are given by $\mu_i(x, y) = x + i(y - x)$ for $x, y \in F$.

Note that all the finite nearfields were determined by Zassenhaus [**7**]. They are the *Dickson nearfields*, which are obtained by 'twisting' the multiplication in a field, and having metacyclic multiplicative group; and seven *exceptional nearfields*, whose multiplicative groups involve $\mathrm{SL}(2, 3)$ or $\mathrm{SL}(2, 5)$.

4. *Rank and nullity*

The structure theory of non-trivial independence algebras splits into two cases, according as $\langle\emptyset\rangle = \emptyset$ or not. We let $C = \langle\emptyset\rangle$, the unique minimal subalgebra, and call the elements of C *constants*. For most of this section, we consider the case where $C \neq \emptyset$.

The *rank* $\mathrm{r}(f)$ of an endomorphism f is equal to the rank of its image. In the case where $C \neq \emptyset$, the *nullity* $\mathrm{n}(f)$ of f is equal to the rank of Cf^{-1}. Our main goal in this section is to verify the 'rank-and-nullity' formula of elementary linear algebra. Note that, if A has rank n, then $\mathrm{r}(f) + \mathrm{n}(f) \leq n$ for any endomorphism f: for if we choose a basis $\{a_1, \ldots, a_m\}$ for the null space of f and extend it to a basis $\{a_1, \ldots, a_n\}$ for A, then $a_{m+1}f, \ldots, a_nf$ generate the range of f. Pre- or post-multiplying any endomorphism by an automorphism doesn't change its rank and nullity. We can use this fact to reduce the general case to that in which f is an idempotent:

LEMMA 4.1. *For any endomorphism f, there is an automorphism g such that $fgf = f$ (so that fg and gf are idempotents).*

Proof. Take a basis $a_1, \ldots, a_r$ for the image of f, and choose elements $b_1, \ldots, b_r$ such that $b_if = a_i$ for $i = 1, \ldots, r$. Then $b_1, \ldots, b_r$ are independent; we can extend both the a_is and the b_is to bases $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$. Let g be the automorphism satisfying $a_ig = b_i$ for $i = 1, \ldots, n$. Then $b_ifgf = b_if$ for $i \leq r$. If $i > r$, then b_if can be expressed in terms of $a_1, \ldots, a_r$ using the operations of the algebra, and the definition of an endomorphism and the fact that $a_ig = b_i$ and $b_if = a_i$ for $i \leq r$ shows that $b_ifgf = b_if$ in this case too.

First, we consider the 2-dimensional case.

LEMMA 4.2. *Let A be a non-trivial independence algebra of dimension 2 with $C \neq \emptyset$. Then $\mathrm{r}(f) + \mathrm{n}(f) = 2$ for any endomorphism f.*

Proof. The result is clear if f is an automorphism, or if the image of f is C. So we may suppose that $\mathrm{r}(f) = 1$. Any subalgebra of dimension 1 except the null space of f is mapped isomorphically onto the image of f. Since A is non-trivial, it has at least three 1-dimensional subalgebras. So there exists a basis a_1, a_2 of A such that $a_1 f = a_2 f$. If f' is another rank 1 endomorphism, and a'_1, a'_2 a basis with $a'_1 f = a'_2 f$, then we can find automorphisms g and h with $a'_i g = a_i$ $(i = 1, 2)$ and $(a_1 f)h = a'_1 f'$; then $gfh = f'$. So all rank 1 endomorphisms have the same nullity. But there is an endomorphism f with $\mathrm{r}(f) = \mathrm{n}(f) = 1$ (choose f to map one element of a basis into C and fix the other).

In order to extend this result to arbitrary dimension, we need some structural information.

PROPOSITION 4.3. *Let A be a non-trivial independence algebra with $C \neq \emptyset$. Then any 2-dimensional subalgebra of A is non-trivial.*

Proof. Let t be chosen such that t-dimensional subalgebras are trivial and $(t+1)$-dimensional subalgebras are not. Assume for a contradiction that $t > 1$. Replacing A by $A[B]$, where B has dimension $t - 2$, we may assume that $t = 2$. Then, replacing A by a subalgebra, we may assume that A has dimension 3.

Let f be an endomorphism of rank 2. There are more than three one-dimensional subalgebras, of which at most one is in the kernel of f. By assumption, the image of f has only two one-dimensional subalgebras. So there are two 1-dimensional subalgebras which have the same image, and hence a basis a_1, a_2, a_3 with $a_1 f = a_2 f$ and with $a_1 f$ and $a_3 f$ independent. As in Lemma 4.2, it follows that all rank 2 endomorphisms are equivalent under pre- and post-multiplication by automorphisms. At least one such endomorphism has nullity 1, and so they all do. But if b is a basis for the kernel of f, then a_1, a_2, b is a basis for A, and so f has rank 1, a contradiction.

THEOREM 4.4. *Let A be a non-trivial independence algebra of dimension n, with $C \neq \emptyset$. Then $\mathrm{r}(f) + \mathrm{n}(f) = n$ for any endomorphism f of A.*

Proof. We know that $\mathrm{r}(f) + \mathrm{n}(f) \leq n$, and must show the reverse inequality. By Lemma 4.1, we may assume that f is an idempotent. Choose a basis $a_1, \ldots, a_r$ for the image of f. We show that we can extend it to a basis $a_1, \ldots, a_n$ of A such that $a_{r+1}, \ldots, a_n$ lie in the null space of f. Suppose that $a_{r+1}, \ldots, a_k$ have been chosen, with $k < n$. Choose an element $b \notin \langle a_1, \ldots, a_k \rangle$. If $bf \in C$, we set $a_{k+1} = b$. Suppose not. Since f is idempotent, $\langle b, bf \rangle$ is a 2-dimensional subalgebra which is invariant under f. By Proposition 4.3, this subalgebra is non-trivial; by Lemma 4.2, it contains an element $b' \notin C$ with $b'f \in C$. Now set $a_{k+1} = b'$. Proceeding in this way, we find the required basis.

Another property of non-trivial algebras is the following:

PROPOSITION 4.5. *Let A be a non-trivial independence algebra with $C \neq \emptyset$. Then, for any 1-dimensional subalgebra B of A, the action of* $\mathrm{Aut}(B)$ *on C defined in Section 2 is transitive.*

Proof. By Proposition 4.3, it suffices to prove this when A has dimension 2. As in Lemma 4.2, all rank 1 endomorphisms are equivalent under pre- and post-multiplication by automorphisms. Such multiplication doesn't change the set

$$\{c \in C : (\exists x \notin C)\; xf = c\},$$

which is an orbit of the group $G = \mathrm{Aut}(B)$, where B is the kernel of f. But every element of C lies in this set for some rank 1 endomorphism f.

To conclude this section, we prove an analogue of Theorem 4.4 for algebras with no constants (in which case, the nullity is undefined).

PROPOSITION 4.6. *Let A be a non-trivial independence algebra of dimension n with $C = \emptyset$. Let f be an endomorphism of A with rank r, and let B be a subalgebra of the image of f with dimension d. Then Bf^{-1} has dimension $d + n - r$.*

Proof. Without loss, f is idempotent. Then $A[B]$ is a non-trivial independence algebra of dimension $n - d$, and f induces an endomorphism of it with rank $r - d$, and hence with nullity $(n-d)-(r-d) = n-r$ (by Theorem 4.4). This means that Bf^{-1} has dimension $n - r$ in the algebra $A[B]$, so its dimension in A is $n - r + d$.

5. *Subalgebra lattices*

THEOREM 5.1. *The subalgebra lattice of a non-trivial independence algebra is isomorphic to the lattice of subspaces of a projective or affine geometry, according as $\langle\emptyset\rangle \neq \emptyset$ or $\langle\emptyset\rangle = \emptyset$.*

Proof. Consider first the case that $\langle\emptyset\rangle \neq \emptyset$. The subalgebra lattice is geometric; we have to prove that it is modular, or equivalently, that

$$\dim(\langle B_1, B_2\rangle) + \dim(B_1 \cap B_2) = \dim(B_1) + \dim(B_2)$$

for any two subalgebras B_1, B_2. By replacing the algebra A by $\langle B_1, B_2\rangle[B_1 \cap B_2]$, we may assume that $\langle B_1, B_2\rangle = A$ and $B_1 \cap B_2 = \langle\emptyset\rangle$. Let A have dimension n and B_i have dimension r_i for $i = 1, 2$. Clearly $r_1 + r_2 \geq n$.

Let f be an endomorphism with image B_1, and g an endomorphism with kernel B_2. Since $B_1 \cap B_2 = C$, the restriction of g to B_1 is an isomorphism; so $\mathrm{r}(fg) \geq \mathrm{r}(f) = r_1$. Clearly $\mathrm{r}(fg) \leq \mathrm{r}(g)$, and so $\mathrm{n}(fg) \geq \mathrm{n}(g) = r_2$. By Theorem 4.4,

$$r_1 + r_2 \leq \mathrm{r}(fg) + \mathrm{n}(fg) = n.$$

Thus equality holds, and the assertion is proved.

Now assume that $\langle\emptyset\rangle = \emptyset$. For any 1-dimensional subalgebra B of A, $\mathrm{Lat}(A[B])$ (the lattice of subalgebras containing B) is a projective space; so, to show that $\mathrm{Lat}(A)$ is an affine space, it suffices to show that its planes are affine planes. Hence we may assume that A has dimension 3, and we must verify Euclid's postulate (where 'points' and 'lines' are subalgebras of dimension 1 and 2 respectively).

Let P be a point, L a line not containing P. Choose a point Q of L, and let M be the line $\langle P, Q\rangle$. Construct an endomorphism f mapping L to Q and P to P. Then f has rank 2 (its image is M), and so Pf^{-1} has dimension 2 (by Proposition 4.6). Hence Pf^{-1} is a line on P parallel to L. Let L' be any other line on P. Then f maps L' isomorphically onto M; so there is a point Q' of L' mapped to Q. But then Q' is on L, and the line L' is not parallel to L.

6. *Geometric groups*

A permutation group G is called *geometric* (Cameron and Deza [**2**]) if it has the property that the pointwise stabilizer of any sequence of points acts transitively on the points it doesn't fix (if any). In a geometric group, the fixed point sets of subgroups are the flats of a matroid (that is, they satisfy the exchange axiom). Hence the *rank* of a geometric group (the cardinality of a minimal set whose pointwise stabilizer is the identity) is well-defined.

A geometric group of rank 1 is just a regular permutation group, possibly with some additional fixed points. Maund [**6**] determined all the finite geometric groups of rank greater than 1. Her proof uses the classification of finite simple groups to determine the rank 2 geometric groups, and then proceeds by induction. An independent determination of the geometric groups of sufficiently large rank (at least 7), not using the classification, is due to Zil'ber [**8**]. Maund's results have not been published (except in her thesis), but a survey of the methods and results in the rank 2 case is given by Cameron [**1**].

The relevance of geometric groups to our problem is given by the next result, whose proof is immediate from the properties of independent sets.

THEOREM 6.1. *The automorphism group of an independence algebra is a geometric group.*

If we are to obtain a complete classification of finite independence algebras, there seems little alternative to using group theory for the rank 2 case, since the geometric approach of Theorem 5.1 gives no information for rank 2. Probably, a more elementary argument could be found for higher rank.

Table 1 gives the list of finite geometric groups of rank 2, taken from Maund [**6**]. In the table, l denotes the number of 1-dimensional subalgebras, and k the cardinality of $B \setminus C$ where $\dim(B) = 1$. (q is a prime power.) The first case in the table corresponds to trivial independence algebras; we consider the remaining cases.

7. *The case $C \neq \emptyset$: dimension 2*

We begin with a counting argument.

PROPOSITION 7.1. *Let A be a finite non-trivial independence algebra of dimension 2. Suppose that the cardinalities of subalgebras of dimensions $0, 1, 2$ are x, $x + k$, $x + kl$ respectively (so that there are l subalgebras of dimension 1). Then*

$$x = \frac{k}{l-2}.$$

Proof. Let $C = \langle\emptyset\rangle$ and let B be a dimension 1 subalgebra. We count endomorphisms $A \to B$ in two ways. Clearly there are $(x + k)^2$ such endomorphisms. Of these, x^2 have rank 0, and lxk have rank 1 (since there are l choices for the kernel B', x choices for the image of a basis element of B', and k choices for the image of a second basis element of A). So $(x + k)^2 = x^2 + lxk$, from which the result follows.

This immediately excludes cases 6, 7, 8, 9 in the table, and shows that $q = 3$ in case 3 and $q \leq 4$ in case 4. Moreover, in Case 3, we have $x = 1$, and this case is an

TABLE 1. *Geometric groups of rank 2*

No.	Group	k	l
1	$H \text{ wr } S_2$	arbitrary	2
2	$M.S_3 \leq H \text{ wr } S_3$ $M = \{(h_1, h_2, h_3) : h_1h_2h_3 = 1\}$ H abelian	arbitrary	3
3	Sharply 2-transitive	1	q
4	$V^2.\mathrm{AGL}(1,q)$ $\dim(V) = d$	q^d	q
5	$V^2.\mathrm{GL}(2,q)$ $\dim(V) = d$	$q^d(q-1)$	$q+1$
6	$Z_{(q-1)/2} \times \mathrm{PSL}(2,q)$ $q \equiv 3 \pmod 4$	$(q-1)/2$	$q+1$
7	$Z_{q-1} \times \mathrm{Sz}(q)$ $q = 2^{2d+1}$	$q-1$	q^2+1
8	$\mathrm{PGL}(3,2)$	2	7
9	$\mathrm{PGL}(3,3)$	6	13

instance of case 5 (with $q = 2$ and $d = 0$). The classification is completed by the following Lemmas.

LEMMA 7.2. *In case 2, $k = 2^d$ and H is elementary abelian, so that this case is an instance of case 5.*

Proof. We have $x = k$. Since H acts transitively on C, and $|C| = |H|$, the action is regular, and we can identify C with H. Now we label the 1-dimensional subalgebras with the three non-zero elements a, b, c of a Klein group K, and label C with the zero of this group. So we can identify A with the set $H \times K$. We write both H and K additively. The subalgebras of A now have the form $H \times L$, where L is a subgroup of K, and the automorphisms have the form

$$(h, x)f = (h + p(x), x\pi), \tag{7.1}$$

where p is a function from K to H satisfying $p(0) = 0$ and $p(a) + p(b) + p(c) = 0$, and π is an automorphism of K. (Recall that the automorphism group of K is the symmetric group S_3 acting on the non-identity elements.)

Now the fact that C is identified with H translates into the assertion that any endomorphism has the form of Equation (7.1), where now π is any endomorphism of K. Moreover, we have $p(0) = 0$, since endomorphisms act trivially on C. There must be a further constraint since, for a given π, there are only k^2 endomorphisms. We denote the endomorphism (7.1) by $f_{p,\pi}$. Now it is easily checked that, if π' is the identity automorphism, then

$$f_{p',\pi'}f_{p,\pi} = f_{p+p',\pi};$$

and any endomorphism with a given π is obtained in this way. So all such endomorphisms have $p(a)+p(b)+p(c)=g(\pi)$, where $g(\pi)$ depends only on π.

Let π be the endomorphism which maps 0 and b to 0, a and c to a. Then we find that, for any endomorphism $f_{p,\pi}$,

$$f_{p,\pi}^2 = fp',\pi,$$

where

$$p'(a)=p(a), \quad p'(b)=0, \quad p'(c)=p(a)+p(c).$$

Thus

$$3p(a)+p(b)+p(c)=g(\pi)=p(a)+p(b)+p(c),$$

so $2p(a)=0$. Since $p(a)$ is an arbitrary element of H, we see that H is an elementary abelian 2-group.

Now, using the fact that $\mathrm{GL}(2,2)\cong S_3$, we see that this case is the subcase $q=2$ of Case 5.

LEMMA 7.3. *Case 4 doesn't occur, except for $q=3$, $|C|=1$.*

Proof. We know that $q\le 4$. If $q=3$, then we have an instance of Case 2. In that case, we showed that $|H|$ is a power of 2. If it is also a power of 3, then it is 1 as claimed.

Suppose that $q=4$, so that $|C|=q/2$. Let f be a rank 0 endomorphism. Then the inverse image of any element of C under f contains two points of $B\setminus C$ for each of the four 1-dimensional subalgebras B. Moreover, the group

$$H=\{g\in \mathrm{Aut}(A) : gf=f\}$$

acts as a rank 2 geometric group on these eight points. From Maund's classification, this group must be $\mathrm{GL}(2,3)$. But this group is not contained in $V^2.\mathrm{AGL}(1,4)$, since its Sylow 2-subgroup is a quaternion group. So this case does not occur.

LEMMA 7.4. *In Case 5, the algebra is equivalent to $V[W]$, where V is a vector space of dimension $d+2$ and W a subspace of codimension 2.*

Proof. The elements of the algebra are the vectors in a $d+2$-dimensional vector space V over $\mathrm{GF}(q)$ with a distinguished d-dimensional subspace W. The subalgebras are the subspaces of V containing W, and the automorphisms are all those represented by matrices of the form

$$\begin{pmatrix} I & O \\ X & A \end{pmatrix},$$

where I is the identity on W (of size $d\times d$), X is an arbitrary $2\times d$ matrix, and $A\in\mathrm{GL}(2,q)$. Moreover, the restriction of any endomorphism to a 1-dimensional subalgebra is a linear map fixing W elementwise.

Now a rank 0 endomorphism has the form $(w,z)f=(w+p(z),0)$ for some function p. Premultiplying f by an automorphism with $A=I$, we see that we can add to p any linear function zX, where X is $2\times d$. This accounts for all the rank 0 endomorphisms, since there are only q^{2d} of them. Now, premultiplying by an automorphism with $X=O$, we see that, for any $A\in\mathrm{GL}(2,q)$, we have $p(zA)=zX$

for some matrix X. Thus, p is linear. Hence the rank 0 endomorphisms are linear. A similar argument shows that the rank 1 endomorphisms are also linear.

8. *The case $C \neq \emptyset$: arbitrary dimension*

Maund's classification of geometric groups of higher rank is based on her result for rank 2: it involves finding all ways of 'fitting together' geometric groups of smaller rank. The task is much easier here, since we have only one type of geometric group of rank 2 to consider, namely case 5 in the table. Maund's methods show that the automorphism group of our algebra will have the form $W^k.\mathrm{GL}(k,q)$, where W is a d-dimensional vector space over $\mathrm{GF}(q)$. The set on which this group acts can be identified with $V \setminus W$, where V is a $(k+d)$-dimensional vector space over $\mathrm{GF}(q)$, and W is a d-dimensional subspace. Moreover, we have $x = q^d$, and the subalgebra $C = \langle\emptyset\rangle$ has the structure of a d-dimensional vector space over $\mathrm{GF}(q)$. So we can identify the whole algebra with V. Under this identification, the subalgebras are the subspaces of V which contain W, and the automorphisms are the automorphisms of V which fix W elementwise. Furthermore, by induction, the restriction of any endomorphism of A to a proper subspace is a vector space endomorphism. Since a map on a vector space is an endomorphism if and only if its restriction to any two-dimensional subspace is an endomorphism, we have shown:

Proposition 8.1. *A non-trivial finite independence algebra with $\langle\emptyset\rangle \neq \emptyset$ is equivalent to $V[W]$, where V is a vector space and W a subspace.*

9. *The case $C = \emptyset$: dimension 2*

In this case, the following result provides a strong restriction.

Proposition 9.1. *Let A be a non-trivial independence algebra of dimension 2, and f an endomorphism of rank 1. Let $H = \{g \in \mathrm{Aut}(A) : gf = f\}$. Then*

(i) the preimage of any element of the image of f is a transversal for the 1-dimensional subalgebras of A;

(ii) H is sharply 2-transitive on each such preimage.

Proof. (i) This holds because f induces an isomorphism on any 1-dimensional subalgebra.

(ii) Let X be the preimage of a point, and let (x_1, x_2) and (y_1, y_2) be pairs of distinct elements of X. Then (x_1, x_2) and (y_1, y_2) are bases, and so there is a unique automorphism g carrying the first to the second. Now gf and f agree on y_1 and y_2; so $gf = f$ and $g \in H$.

We immediately exclude cases 5 (for $q \geq 3$), 6, 7, 8, 9 in the table, since these groups do not contain sharply 2-transitive subgroups. We complete the analysis with the following Lemmas.

Lemma 9.2. *In case 2, $k = 3^d$, H is elementary abelian, and we have an instance of case 4.*

Proof. The elements of the algebra can be represented as pairs (h,i), where $h \in H$ and $i \in \{0,1,2\}$. Automorphisms have the form $(h,i)f = (h+p(i), i\pi)$, where π is a permutation of $\{0,1,2\}$, and $p(0)+p(1)+p(2)=0$.

An endomorphism of rank 1 whose image is $\{(h,0) : h \in H\}$ has the form $(h,i)f = (h+p(i),0)$. As we have seen before, the value of $p(0)+p(1)+p(2)$ is independent of the choice of f. Now

$$(h,i)f^2 = (h+p(i)+p(0),0),$$

so

$$2p(0)+p(0)+p(1)+p(0)+p(2) = p(0)+p(1)+p(2),$$

or $3p(0)=0$. Since $p(0)$ is arbitrary, H is an elementary abelian 3-group. The lemma is proved, since $S_3 \cong \mathrm{AGL}(1,3)$.

LEMMA 9.3. *The independence algebra in case 3 is unique up to equivalence.*

Proof. We know everything except the endomorphisms of rank 1. But such an endomorphism must map A to a single element, since the 1-dimensional subalgebras are singletons.

REMARK. As we saw earlier, a finite sharply 2-transitive group is the affine group of dimension 1 over a nearfield, and the finite nearfields have been determined by Zassenhaus [**7**].

LEMMA 9.4. *In case 4, the algebra is equivalent to* $\mathrm{Aff}(V)[+W]$*, where* V *is a vector space over* $\mathrm{GF}(q)$ *and* W *a subspace of codimension* 1.

Proof. Note first that $q>2$, since the algebra is nontrivial. The set of elements can be taken as a $(d+1)$-dimensional vector space V over $\mathrm{GF}(q)$: we write the vectors in the form (x,z), where $x \in \mathrm{GF}(q)^d$ and $z \in \mathrm{GF}(q)$. The subalgebras are the cosets of the subspace W consisting of vectors with $z=0$, and the automorphisms have the form

$$(x,z)f = (x,z)\begin{pmatrix} I & O \\ u & a \end{pmatrix} + (x',z')$$

with $a \neq 0$. Our job is to determine the endomorphisms of rank 1.

As we have seen, the inverse image of a point under a rank 1 endomorphism f admits a sharply 2-transitive group $\mathrm{AGL}(1,q)$. Now, by the Schur–Zassenhaus Theorem, the subgroups of order $q-1$ of the automorphism group are all conjugate, and we may assume that the sharply transitive group in question contains the subgroup consisting of all transformations in the above form with $u=x'=z'=0$. The orbits of this group on vectors with $z \neq 0$ have the form $\{(x,z) : z \neq 0\}$ for fixed x; they are subsets of affine lines, all parallel. Since $q>2$, a $(q-1)$-element subset of an affine line determines the line uniquely; so the orbits of our $\mathrm{AGL}(1,q)$ are the lines in a parallel class, and f projects along this parallel class: each point p of V is mapped to the intersection of the line of the parallel class containing p with the image of f. Since the number of parallel classes of lines which are transversals to the cosets of W is equal to the number of endomorphisms with given image, we have determined the endomorphisms completely.

LEMMA 9.5. *Case 5 does not occur except for $q = 2$ and $|C| = 1$.*

Proof. We know that $q = 2$. But then we have an instance of Case 2, with H an elementary abelian 2-group. However, we showed that it is also an elementary abelian 3-group. So it is trivial.

10. *The case $C = \emptyset$: arbitrary dimension*

Once again we have only to deal with a special case of Maund's list, because of the restrictions on the rank 2 cases. (We have a transitive geometric group in which the point stabiliser is of the form $W^k.\mathrm{GL}(k,q)$ and the rank 2 subgroups are $W^2.\mathrm{GL}(2,q)$ or sharply 2-transitive.) The only possible groups are $W^k.\mathrm{AGL}(k,q)$, where $\dim(W) = d$, acting on q^{d+k} points. Moreover, the elements of A are those of a vector space V of dimension $d + k$.

We claim that the algebra is equivalent to $\mathrm{Aff}(V)[+W]$, where $\dim(V) = d + k$ and $\dim(W) = d$. Indeed, we know that the subalgebras and automorphisms are correct. Now it suffices to show that any idempotent endomorphism f is an endomorphism of $\mathrm{Aff}(V)[+W]$, since any endomorphism can be made idempotent by multiplying by automorphisms. But an idempotent endomorphism fixes a point, which we may assume lies in W, and so fixes every point of W. Thus, it is an endomorphism of $A[W]$. But we know by our previous analysis that $A[W]$ is equivalent to $V[W]$, so f is an endomorphism of $V[W]$, and hence of $\mathrm{Aff}(V)[+W]$.

To summarise the last two sections:

PROPOSITION 10.1. *A finite non-trivial independence algebra with $\langle\emptyset\rangle = \emptyset$ is equivalent either to $\mathrm{Aff}(V)[+W]$ for some vector space V and subspace W, or to an affine nearfield algebra.*

Combining this with Proposition 8.1, we have proved our main theorem classifying the finite independence algebras.

11. *Further comments*

What about infinite independence algebras of finite dimension? We know that the subalgebra lattice is a Boolean lattice (in the trivial case) or a projective or affine geometry.

This immediately shows, for example, that if an infinite independence algebra has finite dimension, then any subalgebra of dimension at least 2 is infinite. One-dimensional subalgebras may have cardinality 1 (as in algebras from sharply 2-transitive groups, for example). We do not know whether the 1-dimensional subalgebras of an infinite independence algebra of finite dimension can have finite cardinality greater than 1. We conjecture that this cannot happen. No examples are known.

What about infinite dimension? Assuming that A is non-trivial, we know that the interval of $\mathrm{Lat}(A)$ below any algebra of finite dimension is a projective or affine geometry. So the elements of finite dimension in $\mathrm{Lat}(A)$ are those of finite dimension in such a geometry. It follows that $\mathrm{Lat}(A)$ is itself a projective or affine geometry. For any subalgebra is clearly a geometric subspace. Conversely, if B corresponds to a subspace, then for any $x_1, \ldots, x_n \in B$, there is a subspace of finite dimension (and hence a subalgebra) which contains $x_1, \ldots, x_n$ and is contained in B. So B is closed under all operations, and is a subalgebra.

In particular:

THEOREM 11.1. *A non-trivial locally finite infinite independence algebra is equivalent to* $V[W]$ *or* $\mathrm{Aff}(V)[+W]$, *where* V *is an infinite-dimensional vector space over a finite field, and* W *a finite-dimensional subspace.*

Note that this result does not require the Classification of Finite Simple Groups, since only the structure of finite independence algebras of sufficiently large dimension is needed, and for this we may use Zil'ber's proof instead of Maund's.

ACKNOWLEDGEMENTS. The second author was partially supported by Hungarian National Scientific Research Foundation #T023186.

References

1. P. J. CAMERON, Bases in permutation groups, pp. 181–198 in *Automorphisms of First-Order Structures* (ed. R. Kaye and H. D. Macpherson), Oxford University Press, Oxford, 1994.

2. P. J. CAMERON and M. DEZA, On permutation geometries, *J. London Math. Soc.* (2) **20** (1979), 373–386.

3. J. R. CLAY, *Nearrings: Geneses and Applications*, Oxford Univ. Press, Oxford, 1992.

4. J. B. FOUNTAIN and A. M. LEWIN, Products of idempotent endomorphisms of an independence algebra of infinite rank, *Math. Proc. Cambridge Philos. Soc.* **114** 1993), 303–319.

5. V. A. R. GOULD, Independence algebras, *Algebra Universalis* **33** (1995), 294–318.

6. T. MAUND, D. Phil. thesis, Oxford University, 1989.

7. H. ZASSENHAUS, Über endliche Fastkörpe, *Abh. Math. Sem. Hamburg* **11** (1936), 187–220.

8. B. I. ZIL'BER, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.*, (Warsaw 1983).

School of Mathematical Sciences
Queen Mary and Westfield College
Mile End Road
London E1 4NS
U.K.

Department of Algebra and Number Theory
Eőtvős L. University
Muzeum krt. 6–8
H-1088 Budapest
Hungary