QUASIGROUPS, HYPERQUASIGROUPS, AND VECTOR SPACES OVER FIELDS WITH ONE OR MORE ELEMENTS

JONATHAN D.H. SMITH

Abstract. The paper presents an elementary and unified approach to vector spaces over fields of order greater than or equal to one (the latter reducing to sets), based on three key principles. Firstly, use of quasigroups enables the field concept to be redefined in a way that admits a field of order one. Secondly, use of hyperquasigroups provides a recursive definition of linear combination that applies equally well to vector spaces over fields of order greater than or equal to one. Thirdly, it is recognised that relations rather than functions provide the correct morphisms for a category of sets to behave like categories of vector spaces over fields of order greater than one.

Dedicated to L.A. Bokut' on the occasion of his eightieth birthday.

1. Introduction

For various reasons, mathematicians have pondered the existence of a field with one element (compare [2] [3], [4], [6, (0.4.24.2)], [12], [13], [16], [23], [24], for example). The most ambitious motivation for such considerations is the desire to transfer Weil's proof of the Riemann hypothesis for curves over finite fields to a proof of the classical Riemann hypothesis, interpreting $\mathbb{Z}$ as a curve over a field of order one.

The goal of the current paper is much more modest and elementary. The primary motivation is the observation that in algebra, combinatorial structures on sets and linear algebraic structures on vector spaces often appear in parallel, so that it would be desirable to have a fully unified approach that embraces both. One example of such parallel appearance concerns groups over sets and Hopf algebras over vector spaces. A second example appears in the work of Bokut, Chen and Mo [1], juxtaposing Evans' proof that every countably generated semigroup can be embedded into a two-generated semigroup [8] alongside Malcev's proof that every countably

2010 *Mathematics Subject Classification.* 12-01, 15-01, 05A30, 20N05.

Key words and phrases. field, linear combination, quasigroup, hyperquasigroup, Hopf algebra, Gaussian binomial coefficient.

generated associative (linear) algebra can be embedded into a two-generated associative (linear) algebra [17].

We begin by making a small change to the classical definition of a field so that it also embraces a field $\mathsf{GF}(1)$ of order one (Definition 2.8), but admits no other extraneous fields (Theorem 2.11). The new definition involves some rudimentary quasigroup theory, covered in §§2.1–2.3.

Once the field of order one is admitted, the next step is to construe sets as vector spaces, sustaining linear combinations. This is achieved using a new recursive definition of linear combinations (Definition 3.8) which is based on the concept of a linear hyperquasigroup. Hypergroups, which provide a more symmetrical version of quasigroup theory (enlarging left/right duality to triality) are introduced in §3.1. Linear hyperquasigroups are covered in §3.2. On sets, as vector spaces over $\mathsf{GF}(1)$, the recursive step in the new definition of a linear combination is never called. In vector spaces over fields with nonzero elements, on the other hand, the recursive construction of general linear combinations is modeled by parsing trees in linear hyperquasigroups, as illustrated by an example in Figure 2. Theorem 3.15 shows that the new definition of a linear combination agrees with the classical definition over fields with more than one element. Section 3.4 covers spans and subspaces over fields with one or more elements, while §3.5 deals with linear transformations.

One of the major obstacles to developing a theory of sets as vector spaces over a singleton field has been the fact that the category of sets and functions is quite unlike categories of vector spaces. In particular, the latter have biproducts, while coproducts of sets, namely disjoint unions, do not function as products. In the final chapter of the paper, we overcome this obstacle by turning to the category **Rel** of relations between sets, whose properties are summarized in §4.1. A unified treatment of linear algebra, working with the usual categories of finite-dimensional vector spaces in parallel with the category of relations between finite sets, is sketched in §4.2. Finally, in §4.3, unified interpretations of q-numbers, q-factorials and q-binomial coefficients are provided for enumeration questions in vector spaces over $\mathsf{GF}(q)$ for $q \geq 1$.

Readers are generally referred to [22] for those notational conventions and definitions that are not explicitly stated in the paper. While our general preference is for algebraic notation (first the argument, then the function, reading from left to right), the opposite Eulerian notation is used for the discussion of linear transformations in §3.5.

2. Quasigroups, and fields with one or more elements

2.1. **Combinatorial quasigroups.** Let $(Q, \cdot)$ be a magma, a (possibly empty) set Q equipped with a binary operation $x \cdot y$ or xy of *multiplication.*

For each element q of Q, define the *left multiplication*

$$L(q)\colon Q \to Q; x \mapsto q \cdot x \tag{2.1}$$

and *right multiplication*

$$R(q)\colon Q \to Q; x \mapsto x \cdot q\,. \tag{2.2}$$

The algebra $(Q, \cdot)$ is said to be a (*combinatorial*) *quasigroup* if all the left and right multiplications are permutations of Q.

Example 2.1. (a) A group $(Q.\cdot)$ is a non-empty quasigroup satisfying the associative law $xy \cdot z = x \cdot yz$. The associative law is expressed here with the governing convention that multiplications denoted by juxtaposition bind more strongly than explicitly written multiplications.

(b) The empty quasigroup $(\varnothing, \cdot)$ vacuously satisfies the associative law.

2.2. **Equational quasigroups.** The combinatorial specification of a quasigroup does not admit the use of universal algebraic techniques. For example, a combinatorial quasigroup $(Q, \cdot)$ may be the domain of a magma homomorphism $f\colon (Q, \cdot) \to (P, \cdot)$ whose image is not a combinatorial quasigroup, in violation of the First Isomorphism Theorem [22, Ch. I, Ex. 2.2.1]. In 1949, Evans [7] redefined quasigroups in the form of *equational quasigroups*, namely universal algebras $(Q, \cdot, /, \backslash)$ equipped with three binary operations of multiplication, *right division* / and *left division* \ satisfying the identities

$$\begin{array}{ll|ll} \text{(IL)} & \mathsf{v}\backslash(\mathsf{v}\cdot\mathsf{w}) = \mathsf{w} & \mathsf{w} = (\mathsf{w}\cdot\mathsf{v})/\mathsf{v} & \text{(IR)}\,; \\ \text{(SL)} & \mathsf{v}\cdot(\mathsf{v}\backslash\mathsf{w}) = \mathsf{w} & \mathsf{w} = (\mathsf{w}/\mathsf{v})\cdot\mathsf{v} & \text{(SR)}\,. \end{array}$$

The identities (IL), (IR) serve to yield the injectivity of the left and right multiplications, while (SL), (SR) give their surjectivity.

It is important to observe the symmetry of the equational quasigroup identities about the vertical line separating left from right. In other words, the theory of equational quasigroups possesses a left/right or chiral duality symmetry.

An equational quasigroup $(Q, \cdot, /, \backslash)$ yields a combinatorial quasigroup $(Q, \cdot)$. Conversely, a combinatorial quasigroup $(Q, \cdot)$ yields an equational quasigroup $(Q, \cdot, /, \backslash)$ with divisions $x/y = xR(y)^{-1}$ and $x\backslash y = yL(x)^{-1}$.

Example 2.2. Let G be a group generated by a subset $\{R, L\}$ with at most two elements. Let M be a right G-module. Then a quasigroup structure is defined on M by $x \cdot y = xR + yL$. Quasigroups $(M, \cdot)$ of this type are described as being *linear.* The quasigroup structure, in combination with identification of 0 in M, serves to specify the module together with the G-action. Note that $xR = x \cdot 0$ and $yL = 0 \cdot y$ for $x, y \in M$. Then $x + y = (x/0) \cdot (0\backslash y)$ and $-y = 0/[0\backslash(y \cdot 0)]$.

Equational quasigroups form a variety in the sense of universal algebra, so the images of equational quasigroups, under homomorphisms of equational quasigroups, are themselves equational quasigroups [22, p. 314]. Evans' reformulation of the quasigroup concept opened up combinatorial questions about quasigroups and Latin squares to analysis with algebraic techniques [9]. In particular, we may note the following.

Lemma 2.3. *Suppose that $\theta\colon (Q,\cdot)\to(Q',\cdot)$ is a magma homomorphism between combinatorial quasigroups. Then $\theta\colon (Q,\cdot,/,\backslash)\to(Q',\cdot,/,\backslash)$ is a homomorphism of equational quasigroups.*

Proof. By (SR), the relation $x=(x/y)\cdot y$ holds for all $x,y\in Q$. Thus the relation $x^\theta=(x/y)^\theta\cdot y^\theta$ holds in $(Q',\cdot)$, so that

$$x^\theta/y^\theta=[(x/y)^\theta\cdot y^\theta]/y^\theta=(x/y)^\theta$$

by (SR) in Q', and θ preserves right division. The proof that θ preserves left division follows by chiral duality. □

2.3. **Cayley's Theorem.** Example 2.1(a) noted that groups are associative quasigroups. As shown by Example 2.1(b), the converse statement is false. Nevertheless, it is almost true.

Proposition 2.4 (Cayley's Theorem)**.** *A nonempty associative quasigroup is isomorphic to a permutation group.*

Proof. Let $(Q,\cdot,/,\backslash)$ be a nonempty associative quasigroup. Consider the right multiplication function

$$R\colon Q\to Q!;y\mapsto R(y) \tag{2.3}$$

from Q to the group $Q!$ of all permutations of the set Q. Then the function is injective, since $R(y)=R(z)$ for $y,z\in Q$ implies

$$y=x\backslash(xy)=x\backslash[xR(y)]=x\backslash[xR(z)]=x\backslash(xz)=z$$

by (IL), using an arbitrary element x of the nonempty set Q.

The associative law $xy\cdot z=x\cdot yz$ in Q may be formulated as

$$\forall\ x,y,z\in Q\,,\ xR(y)R(z)=xR(yz)$$

or

$$\forall\ y,z\in Q\,,\ R(y)R(z)=R(yz)\,,$$

so the right multiplication map (2.3) is a magma homomorphism. Then by Lemma 2.3, it is a homomorphism of equational quasigroups. The First Isomorphism Theorem for equational quasigroups shows that the domain Q of the injective right multiplication homomorphism (2.3) is isomorphic to its image, a subgroup of $Q!$. □

Corollary 2.5. *A nonempty associative quasigroup is a group.*

Remark 2.6. Suppose that Q is the empty (associative) quasigroup. Then the right multiplication map (2.3) is the insertion $\emptyset \hookrightarrow \{1_\emptyset\}$. As such, it is an injective quasigroup homomorphism, whose image is the empty subquasigroup of the singleton group $\emptyset!$.

2.4. **Fields with one or more elements.** The classical definition of a field may be encapsulated as follows.

Definition 2.7. A *field* is a commutative ring, in which the set of nonzero elements forms a group under the ring multiplication.

Here, "ring" may denote a nonunital or unital ring, respectively meaning without or with the requirement for a multiplicative identity in the ring. Indeed, the multiplicative identity for the ring is imposed (along with the equation $0 \cdot 1 = 0$) directly by the group requirement in Definition 2.7. The "classical" Definition 2.7 will now be replaced by the following.

Definition 2.8. A *field* is a commutative ring, in which the set of nonzero elements forms a quasigroup under the ring multiplication.

Proposition 2.9. *Under Definition 2.8, the one-element commutative ring* $\mathsf{GF}(1)$ *is a field.*

Proof. Since $\mathsf{GF}(1) = \{0\}$, the set of nonzero elements of $\mathsf{GF}(1)$ is empty. As such, it forms a quasigroup. □

Remark 2.10. While some authors have previously insisted on a distinction $0 \neq 1$ between the additive and multiplicative identities of a unital ring, it should be noted that such inequalities are incompatible with the algebraic nature of the unital ring concept.

We now observe that the new Definition 2.8 does not make any change to the specification of fields with more than one element.

Theorem 2.11. *Let F be a set of cardinality greater than one. Then F is a field in the sense of Definition 2.8 if and only if it is a field in the sense of Definition 2.7.*

Proof. If F is a field in the sense of Definition 2.7, Examole 2.1(a) shows that it is a field in the sense of Definition 2.8. Conversely, suppose that F is a field in the sense of Definition 2.8. Consider the set Q of nonzero elements of F. Since $|F| > |\{0\}|$, the set Q is nonempty. By Definition 2.8, Q is a nonempty, commutative, associative quasigroup. By Corollary 2.5, Q is a group. Then F is a field in the traditional sense of Definition 2.7. □

3. Hyperquasigroups and linear combinations

3.1. **Hyperquasigroups.** As observed in §2.2, the equational theory of quasigroups is endowed with the two-fold symmetry of left/right duality. This symmetry was exploited in Evans' solution of the word problem for quasigroups [7]. Nevertheless, his solution still left many separate cases to consider, at least in principle. Subsequently, the solution of the word problem was drastically simplified by the explicit use of a stronger triality symmetry or S_3-action[1] that interchanges all three equational quasigroup operations and their opposites [19]. While this triality symmetry is already implicit in the theory of equational quasigroups, and its presence had long been recognized, the choice of specific operations in the equational theory was an impediment to its use in practice. Indeed, implementation of the symmetry entailed the introduction of a new approach to quasigroups, by means of the concept of a hyperquasigroup [18, 20]. Hyperquasigroups may be considered as a further step beyond the progression from combinatorial quasigroups to equational quasigroups. They involve the auxiliary concept of a reflexion-inversion space:

Definition 3.1. A *reflexion-inversion space* (Ω, σ, τ) is a set Ω equipped with two involutive actions, a *reflexion*

$$\sigma : \Omega \to \Omega; \omega \mapsto \sigma\omega \tag{3.1}$$

and an *inversion*

$$\tau : \Omega \to \Omega; \omega \mapsto \tau\omega\,. \tag{3.2}$$

Example 3.2. The most basic reflexion-inversion space is the symmetric group $S_3 = \{1, 2, 3\}!$, with reflexion and inversion implemented as the left multiplications by the respective transpositions $(1\ 2)$ and $(2\ 3)$. In this context, it is convenient to identify each element of S_3 as the image of the identity permutation under the left action of a series of reflexions and inversions.

Definition 3.3. A *hyperquasigroup* (Q, Ω) is a pair consisting of a set Q and a reflexion-inversion space Ω, together with a binary action

$$Q^2 \times \Omega \to Q; (x, y, \omega) \mapsto xy\,\underline{\omega} \tag{3.3}$$

of Ω on Q, such that the *hypercommutative law*

$$xy\,\underline{\sigma\omega} = yx\,\underline{\omega} \tag{3.4}$$

[1] This triality symmetry was identified in [19] as *syntactic triality*. That paper also discussed *semantic triality*, which is more closely related to the triality symmetry of Moufang loops and the Coxeter-Dynkin diagram of type D_4 (compare [5]).

and the *hypercancellation law*

$$x\,(xy\,\underline{\omega}\,)\,\underline{\tau\omega} = y \tag{3.5}$$

are satisfied for all x, y in Q and ω in Ω.

Definition 3.3 may be expressed in graphical form. Suppose that (Q, Ω) is a hyperquasigroup. For elements x of Q and ω of Ω, define the (*left*) *translation*

$$L_\omega(x) : Q \to Q; y \mapsto xy\underline{\omega} \tag{3.6}$$

and *right translation*

$$R_\omega(x) : Q \to Q; y \mapsto yx\underline{\omega} \tag{3.7}$$

by analogy with (2.1) and (2.2). Note that

$$R_\omega(x) = L_{\sigma\omega}(x) \tag{3.8}$$

by hypercommutativity, and

$$L_\omega(x)^{-1} = L_{\tau\omega}(x) \tag{3.9}$$

by hypercancellativity. The relation (3.9) serves to justify the use of the term "inversion" for τ in Definition 3.1.

Definition 3.3 is then summarized by the diagram

$$\begin{tikzcd}
 & y \arrow[dr, "R_{\sigma\omega}(x)"] & \\
x \arrow[ur, "R_{\tau\omega}(z)"] \arrow[rr, "R_\omega(y)"'] & & z
\end{tikzcd}$$

(3.10)

in terms of the right translations, or by the diagram

$$\begin{tikzcd}
 & y \arrow[dr, "L_{\sigma\omega}(x)"] & \\
x \arrow[ur, "L_{\sigma\tau\sigma\omega}(z)"] \arrow[rr, "L_\omega(y)"'] & & z
\end{tikzcd}$$

(3.11)

using left translations, with ω in Ω and x, y, z in Q. For example, the bottom line of (3.10) gives $z = xy\underline{\omega}$. The right leg then yields the hypercommutativity (3.4), while the left leg yields the hypercancellativity (3.5). The equivalence of (3.10) with (3.11) follows by replacement of ω with $\sigma\omega$, and use of (3.8).

The theory of quasigroups is embedded in the theory of hyperquasigroups, as described by the following two results which pass back and forth between quasigroups and hyperquasigroups.

Proposition 3.4. [18, Prop. 5.2] *Let $(Q, \cdot, /, \backslash)$ be an equational quasigroup. Let Ω be the symmetric group S_3, interpreted as a reflexion-inversion space according to Example 3.2. Setting*

$$xy\,\underline{(1)} = x \cdot y\,, \quad xy\,\underline{(13)} = x/y\,, \quad xy\,\underline{(23)} = x\backslash y\,,$$
$$xy\,\underline{(12)} = y \cdot x\,, \quad xy\,\underline{(123)} = y/x\,, \quad xy\,\underline{(132)} = y\backslash x\,,$$

the pair (Q, Ω) becomes a hyperquasigroup.

Theorem 3.5. [18, Th. 6.1, Cor. 6.2] *Let (Q, Ω) be a hyperquasigroup. Then for each element ω of the reflexion-inversion space Ω, there is an equational quasigroup $(Q, \underline{\sigma\omega}\,, \underline{\sigma\tau\omega}\,, \underline{\tau\sigma\omega}\,)$. In particular, for each element ω of the reflexion-inversion space Ω, there is a combinatorial quasigroup $(Q, \underline{\omega})$.*

Theorem 3.5 exhibits a typical phenomenon whereby a reflexion-inversion space is a moduli space for a collection of quasigroup structures.

3.2. **Linear hyperquasigroups.** In Example 2.2, it was shown how linear representations of two-generated groups may be captured by a quasigroup structure. We will now discuss how certain hyperquasigroups are able to capture linear representations of arbitrary groups.

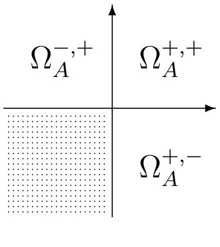

FIGURE 1. Orthant structure

Let A be an arbitrary group of automorphisms of an abelian group (or right A-module) M. Define sets

$$\left\{\begin{aligned} \Omega_A^{+,+} &= A \times A\,, \\ \Omega_A^{-,+} &= (-A) \times A\,, \\ \Omega_A^{+,-} &= A \times (-A)\,, \end{aligned}\right. \tag{3.12}$$

known respectively as the *positive cone* or *first* or 2^0-*th orthant*, the *second* or 2^1-*st orthant*, and the the *fourth* or 2^2-*nd orthant.* The orthant notation is motivated by the case where M is the real line, and A is the group of positive scalars (see Figure 1.) Define

$$\Omega_A = \Omega_A^{+,+} \cup \Omega_A^{-,+} \cup \Omega_A^{+,-}\,. \tag{3.13}$$

Define a reflexion

$$\sigma : \Omega_A \to \Omega_A; (r,s) \mapsto (s,r) \tag{3.14}$$

and an inversion

$$\tau : \Omega_A \to \Omega_A; (r,s) \mapsto (-rs^{-1}, s^{-1}) \tag{3.15}$$

to make Ω_A a reflexion-inversion space. The actions of the reflexion and inversion on the orthants are given by the following Cayley diagram:

$$\begin{tikzcd}
\Omega_A^{+,-} \arrow[loop left, dash, "\tau"] \arrow[r, dash, "\sigma"] & \Omega_A^{-,+} \arrow[r, dash, "\tau"] & \Omega_A^{+,+} \arrow[loop right, dash, "\sigma"]
\end{tikzcd}$$

(3.16)

The inherent triality symmetry is given explicitly here by the elements σ and τ generating S_3. At the elementary level, the Cayley diagram appears as follows:

$$\begin{tikzcd}
(r,s) \arrow[r, dash, "\tau"] \arrow[d, dash, "\sigma"'] & (-rs^{-1}, s^{-1}) \arrow[r, dash, "\sigma"] & (s^{-1}, -rs^{-1}) \arrow[d, dash, "\tau"] \\
(s,r) \arrow[r, dash, "\tau"'] & (-sr^{-1}, r^{-1}) \arrow[r, dash, "\sigma"'] & (r^{-1}, -sr^{-1})
\end{tikzcd}$$

For (r,s) in Ω_A, define a binary action on M by

$$xy\,\underline{(r,s)} = xr + ys \tag{3.17}$$

for x, y in M.

Definition 3.6. A hyperquasigroup is said to be *linear* if it has the form (M, Ω_A), its structure being given by (3.14)–(3.17), for a group A of automorphisms of an abelian group M. It is *pointed* if Ω_A is pointed by $(1, 1)$.

Pointed linear hyperquasigroups turn out to be equivalent to faithful group representations (as automorphisms of an abelian group). Indeed, the abelian group M, automorphism group A, and action of A on M are all recovered from the pointed linear hyperquasigroup structure (M, Ω_A).

Theorem 3.7. [21, Th. 11.5] *Consider a pointed linear hyperquasigroup* (M, Ω_A). *Then:*

(a) *The addition and subtraction in the abelian group M are given by*

$$x + y = xy\,\underline{(1, 1)}$$

and

$$x - y = xy\,\underline{(1, -1)} = xy\,\underline{\sigma\tau(1, 1)}$$

for x, y in M, using the pointed element $(1, 1)$ of Ω_A;

(b) *The zero element of M is given as*

$$0 = xy\,\underline{(1, -1)} = xx\,\underline{\sigma\tau(1, 1)} \tag{3.18}$$

for any element x of M, using the pointed element $(1, 1)$ of Ω_A;

(c) *The set*

$$P = \{L_{(r,s)}(x) \mid (r, s) \in \Omega_A^{+,+}\ ,\ x \in M\}$$

of left translations from the positive cone forms a group;

(d) *The group A is the stabilizer P_0 of 0 in the action of P on M;*

(e) *For elements m of M and a of A, the equation*

$$ma = 0m\,\underline{(1, a)}$$

gives the action of a on m.

3.3. **Linear combinations.** Vector spaces are naturally understood as sets that are equipped with an algebraic structure given by linear combinations. In particular, vector spaces over $\mathsf{GF}(1)$ will be sets, and one is left with the question of the appropriate linear combinations.[2] Now there are various ways to define linear combinations. A recursive definition is chosen here, based on the use of an appropriate linear hyperquaisgroup.

Definition 3.8. Let V be a vector space over a field F, with associative, commutative quasigroup F^* of nonzero elements. If $|F| > 1$, consider the linear hyperquasigroup (V, Ω_{F^*}) obtained from the multiplication action of

[2] Compare Cohn's observation: "I know of no ... way to make sense of vector spaces over $\mathbb{F}_1$" [3, p.489].

nonzero scalars. Then an *F-linear combination* of vectors from V is defined recursively as follows:

(a) Each vector $v \in V$ is an F-linear combination of vectors from V;
(b) If x, y are F-linear combinations of vectors from V, and α, β are nonzero elements of F, then $x\alpha + y\beta = xy\,\underline{(\alpha, \beta)}$ is an F-linear combination of vectors from V.

Since there are no nonzero elements of the field $\mathsf{GF}(1)$, the recursive step of Definition 3.8(b) is never called when $F = \mathsf{GF}(1)$. Thus each set is a vector space over $\mathsf{GF}(1)$. To investigate the import of the F-linear combinations of Definition 3.8 for traditional fields, some additional concepts are needed.

Definition 3.9. Let V be a vector space over a field F. Then the *support*, *scalar list*, and *argument list* of an F-linear combination of vectors from V are defined recursively as follows:

(a) For each vector $v \in V$, the support of the F-linear combination v is $\{v\}$, its scalar list is (1), and its argument list is (v);
(b) Suppose that x and y are F-linear combinations of vectors from V with respective supports X, Y; scalar lists $(\alpha_1, \dots \alpha_r), (\beta_1, \dots \beta_s)$; and argument lists $(x_1, \dots, x_r), (y_1, \dots, y_s)$. For nonzero elements α, β of F, the support of the F-linear combination $x\alpha + y\beta$ is $X \cup Y$. Its scalar list is $(\alpha_1\alpha, \dots, \alpha_r\alpha, \beta_1\beta, \dots, \beta_s\beta)$, and its argument list is $(x_1, \dots, x_r, y_1, \dots, y_s)$.

Figure 2 illustrates the recursive construction of F-linear combinations, along with their scalar and argument lists, in a (traditional) field F where $6 \neq 0$. If the underlying vector space is V, then the tree structure of Figure 2 reflects a parsing tree in the linear hyperquasigroup (V, Ω_{F^*}) obtained from the multiplication action of nonzero scalars.

The proof of the following result (by induction on the positive integer r) is left to the reader.

Lemma 3.10. *Let v be an F-linear combination of vectors from V, with support X, scalar list $(\alpha_1, \dots, \alpha_r)$, and argument list $(v_1, \dots, v_r)$.*

(a) *The support is nonempty, while the scalar and argument lists always have positive length r.*
(b) *The support X is the set $\{v_1, \dots, v_r\}$ of vectors appearing (possibly repeatedly) in the argument list.*

Definition 3.11. Suppose that X is a nonempty subset of a vector space V over a field F. Then a vector v is an *F-linear combination of X-vectors* if it appears as an F-linear combination whose support is a nonempty subset of X.

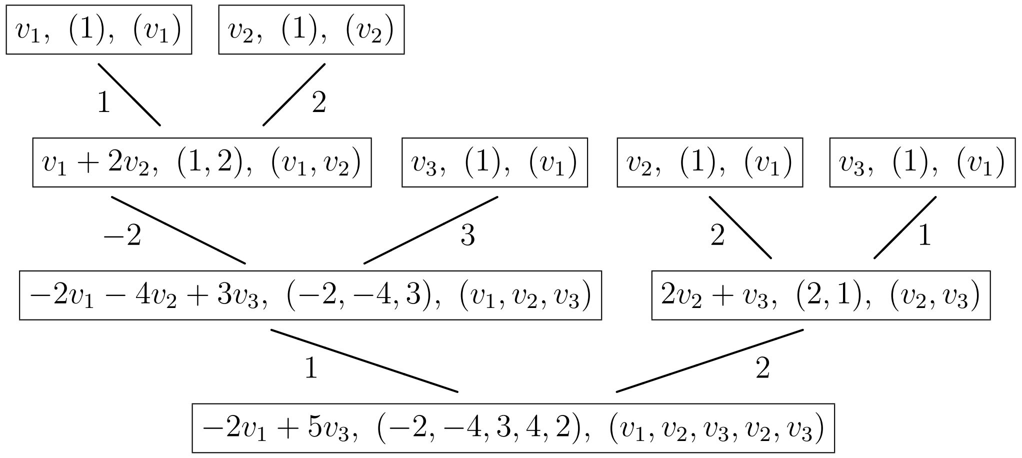
$v_1,\ (1),\ (v_1)$
$v_2,\ (1),\ (v_2)$
1
2
$v_1+2v_2,\ (1,2),\ (v_1,v_2)$
$v_3,\ (1),\ (v_1)$
$v_2,\ (1),\ (v_1)$
$v_3,\ (1),\ (v_1)$
-2
3
2
1
$-2v_1-4v_2+3v_3,\ (-2,-4,3),\ (v_1,v_2,v_3)$
$2v_2+v_3,\ (2,1),\ (v_2,v_3)$
1
2
$-2v_1+5v_3,\ (-2,-4,3,4,2),\ (v_1,v_2,v_3,v_2,v_3)$

FIGURE 2. Recursive construction of F-linear combinations of vectors $v_1, v_2, \ldots$ over a traditional field F with $6 \neq 0$. The nodes of the tree show respective linear combinations (written with left scalar action to conserve space), scalar lists, and argument lists. The edges of the tree are labeled with nonzero scalars from the field. Over $\mathsf{GF}(1)$, the only possible "trees" are isolated leaves of the form $\boxed{v,\ (1),\ (v)}$.

Lemma 3.12. *Suppose that Y is a nonempty subset of a subset X of a vector space V over a field F. If a vector v is an F-linear combination of Y-vectors, then it is an F-linear combination of X-vectors.*

For fields with more that one element, the definitions given here may be compared with the classical definition:

Definition 3.13. [10, §6] Let V be a vector space over a field F with $|F| > 1$. Let r be a natural number. Suppose that

$$v = \sum_{i=1}^{r} v_i \alpha_i \tag{3.19}$$

for a vector v in V, a subset $\{v_1, \ldots, v_r\}$ of V, and a subset $\{\alpha_1, \ldots, \alpha_r\}$ of F. Then v is said to be a *classical linear combination* of the set $\{v_1, \ldots, v_r\}$ of vectors.

Remark 3.14. Consider the situation of Definition 3.13. If r is the natural number 0, then the vector v of (3.19) is the zero vector in V [10, p.9].

The following theorem describes the relationship between the classical and new definitions of a linear combination.

Theorem 3.15. *Let V be a vector space over a field F with $|F| > 1$.*

(a) *The zero vector 0 of V is an F-linear combination of $\{0\}$-vectors.*
(b) *In the situation of Definition 3.13, with r positive, the vector v is an F-linear combination of $\{v_1, \dots, v_r\}$-vectors.*
(c) *Each F-linear combination of vectors from V may be written as a classical linear combination (3.19) of its support.*

Proof. (a) The statement follows by Definition 3.9(a).

(b) The proof is by induction on r. For the induction basis, suppose that $r = 1$. If $\alpha_1 = 1$, then v is simply the F-linear combination $v = v_1$ with support $\{v_1\}$. If $\alpha_1 \neq 1$, then v may be written as the F-linear combination $v = v_1(1)+v_1(\alpha_1-1) = v_1v_1\,\underline{(1, \alpha_1 - 1)}$ with support $\{v_1\}$. For the induction step, suppose that $r \geq 2$, and that the result is true for expressions (3.19) with a positive number of summands that is less than r. Then

$$v = \sum_{i=1}^{r} \alpha_i v_i = \sum_{i=1}^{r-1} \alpha_i v_i + \alpha_r v_r \,.$$

Now $\sum_{i=1}^{r-1} \alpha_i v_i$ is an F-linear combination whose support is a nonempty subset Z of $\{v_1, \dots, v_{r-1}\}$, by the induction assumption. If $\alpha_r = 0$, the induction step is then complete. Otherwise, for $\alpha_r \neq 0$, the vector v_r is itself an F-linear combination with support $\{v_r\}$, and then

$$v = \sum_{i=1}^{r-1} v_i\alpha_i(1) + v_r(\alpha_r) = \left(\sum_{i=1}^{r-1} v_i\alpha_i\right) v_r\,\underline{(1, \alpha_r)}$$

is an F-linear combination whose support is the nonempty subset $Z \cup \{v_r\}$ of $\{v_1, \dots, v_r\}$.

(c) Suppose that v is an F-linear combination of vectors with scalar and argument lists of length r. The result will be proved by induction on r. If $r = 1$, then $\alpha_1 = 1$, and (3.19) holds with $v_1 = v$. Now suppose that $r > 1$, and that the result is true for all F-linear combinations with scalar and argument lists of lengths less than r. Then $v = x\alpha + y\beta$ for nonzero scalars α, β and F-linear combinations x, y with respective scalar lists $(\alpha'_1, \dots, \alpha'_s)$, $(\beta'_1, \dots, \beta'_t)$ and argument lists $(v_1, \dots, v_s)$, $(w_1, \dots, w_t)$ of positive lengths s, t summing to r. By the induction hypothesis, there are classical linear combinations

$$x = \sum_{i=1}^{s} v_i\alpha'_i \quad \text{and} \quad y = \sum_{j=1}^{t} w_j\beta'_j$$

for the subsets $\{v_1, \dots, v_s\}$, $\{w_1, \dots, w_t\}$ of V and $\{\alpha'_1, \dots, \alpha'_s\}$, $\{\beta'_1, \dots, \beta'_t\}$ of F. Then the computation

$$v = x\alpha + y\beta = \sum_{i=1}^{s} v_i\alpha'_i\alpha + \sum_{j=1}^{t} w_j\beta'_j\beta = \sum_{i=1}^{s} v_i(\alpha'_i\alpha) + \sum_{j=1}^{t} w_j(\beta'_j\beta)$$

expresses the F-linear combination v with support $\{v_1, \dots, v_s\} \cup \{w_1, \dots, w_t\}$ as a classical linear combination of $\{v_1, \dots, v_s\} \cup \{w_1, \dots, w_t\}$. □

3.4. **Spans and subspaces.**

Definition 3.16. Let V be a vector space over a field F.

(a) If $|F| > 1$, the *span* $\operatorname{Span} \emptyset$ of the empty set is $\{0\}$.
(b) If $|F| = 1$, the *span* $\operatorname{Span} \emptyset$ of the empty set is $\emptyset$.
(c) Let X be a nonempty subset of V. Then the *span* $\operatorname{Span} X$ of X is the set of all F-linear combinations of X-vectors.

Lemma 3.17. *Let X be a subset of a vector space V over a field F. Then $X \subseteq \operatorname{Span} X$.*

Lemma 3.18. *Let V be a vector space over a field F with $|F| > 1$. Then the zero vector 0 of V lies in the span of every nonempty subset of V.*

Proof. Consider an element v of a nonempty subset X of V. Then using the pointed element $(1, 1)$ of Ω_{F^*}, the relation

$$0 = v(1) + v(-1) = vv\,\underline{(1, -1)} = vv\,\underline{\sigma\tau(1, 1)}$$

corresponding to (3.18) serves to express 0 as an F-linear combination whose support is the nonempty subset $\{v\}$ of X. □

Definition 3.19. Let V be a vector space over a field F.

(a) A subset S of V is a (*vector*) *subspace* if $S = \operatorname{Span} S$.
(b) If $|F| > 1$, a subset S of V is a *classical subspace* if and only if it contains each classical linear combination of each finite subset of S.

Theorem 3.20. *Let V be a vector space over a field F.*

(a) *If $|F| = 1$, then each subset of V is a subspace.*
(b) *If $|F| > 1$, then a subset of V is a subspace if and only if it is a classical subspace.*

Proof. (a) Let S be a subset of V. If $S = \emptyset$, then Definition 3.16(b) implies that $\emptyset = \operatorname{Span} \emptyset$, so S is a subspace. If S is nonempty, the recursive step Definition 3.8(b) is never called when F-linear combinations are formed, so the only F-linear combinations of S-vectors are the elements of S itself, and $S = \operatorname{Span} S$.

(b) Suppose that $S = \operatorname{Span} S$ for a subset S of V. By Definition 3.16(a), S is nonempty, since $\emptyset \neq \operatorname{Span} \emptyset$. Then by Lemma 3.18, the zero vector, namely the unique classical linear combination of the empty subset of S, lies in S. Now consider a classical linear combination (3.19) of a nonempty, finite subset $\{v_1, \dots, v_r\}$ of S. By Theorem 3.15(b), it follows that this classical linear combination v may be expressed as an F-linear combination of $\{v_1, \dots, v_r\}$-vectors. By Lemma 3.12, it follows that v is an F-linear combination of S-vectors, and so lies in S. Thus S is a classical subspace.

Conversely, suppose that S is a classical subspace. Let v be an element of $\operatorname{Span} S$, namely an F-linear combination with support $\{v_1, \dots, v_r\} \subseteq S$. By Theorem 3.15(c), v is a classical linear combination of $\{v_1, \dots, v_r\}$. Then since S is a classical subspace, v lies in S. Conversely, $S \subseteq \operatorname{Span} S$ by Lemma 3.17. Thus $S = \operatorname{Span} S$, and S is a subspace. □

3.5. **Linear transformations.** In this section, linear transformations are defined for fields with one or more elements. It is convenient to use Eulerian rather than algebraic notation for these linear transformations here, so that the preservation of scalar multiplications appears as the mixed associative law in the second equation of (3.20).

Definition 3.21. Let U and V be vector spaces over a field F.

(a) A function $f\colon U \to V$ is said to be a *linear transformation* if, whenever an element u of U is an F-linear combination with scalar list $(\alpha_1, \dots, \alpha_r)$, with argument list $(u_1, \dots, u_r)$, and with support $\{u_1, \dots, u_r\} \subseteq U$, then $f(u)$ is an F-linear combination with scalar list $(\alpha_1, \dots, \alpha_r)$ and argument list $\big(f(u_1), \dots, f(u_r)\big)$.

(b) The spaces U and V are *linearly isomorphic* if there is a bijective linear transformation $f\colon U \to V$.

Theorem 3.22. *Let $f\colon U \to V$ be a function between vector spaces U, V over a field F.*

(a) *If $|F| = 1$, then f is a linear transformation.*

(b) *If $|F| > 1$, then f is a linear transformation if and only if*

$$f(u_1 + u_2) = f(u_1) + f(u_2) \quad \text{and} \quad f(u\alpha) = f(u)\alpha \tag{3.20}$$

for all u, u_1, u_2 in U and α in F.

Proof. (a) If $U = \emptyset$, then the linear transformation condition is satisfied vacuously. Now suppose that U is nonempty. Then an element u of the vector space U appears as an F-linear combination only with scalar list (1) and argument list (u). Since $f(u)$ appears as an F-linear combination with scalar list (1) and argument list $\big(f(u)\big)$, it follows that $f\colon U \to V$ is a linear transformation.

(b) First, suppose that $f\colon U \to V$ is a linear transformation. For vectors u_1, u_2 in U, the vector $u' = u_1 + u_2$ in U is an F-linear combination with scalar list $(1,1)$ and argument list (u_1, u_2), so the vector $f(u')$ in V is an F-linear combination with scalar list $(1,1)$ and argument list $\big(f(u_1), f(u_2)\big)$. It follows that $f(u_1 + u_2) = f(u_1) + f(u_2)$.

Now consider a vector u in U and a scalar α in F. For $\alpha = 1$, one has $f(u\alpha) = f(u) = f(u)\alpha$. For $\alpha \neq 1$, the vector $u\alpha$ is an F-linear combination with scalar list $(1, \alpha - 1)$ and argument list (u, u). Then $f(u\alpha)$ is an F-linear combination with scalar list $(1, \alpha - 1)$ and argument list $\big(f(u), f(u)\big)$. It follows that $f(u\alpha) = f(u) + f(u)(\alpha - 1) = f(u)\alpha$, so the equations (3.20) are satisfied.

Conversely, suppose that the equations (3.20) are satisfied. The linear transformation conditions of Definition 3.21(a) are shown to be satisfied by induction on the length r of the scalar and argument lists in an F-linear combination u. The induction basis $r = 1$ is trivial. For the induction step, suppose that an element u of U is an F-linear combination with scalar list $(\alpha_1\alpha, \dots, \alpha_s\alpha, \beta_1\beta, \dots, \beta_t\beta)$, with argument list $(u_1, \dots, u_s, v_1, \dots, v_t)$, and support $\{u_1, \dots, u_s, v_1, \dots, v_t\} \subseteq U$. Consider the element x of U with scalar list $(\alpha_1, \dots, \alpha_s)$ and argument list $(u_1, \dots, u_s)$, along with the element y of U with scalar list $(\beta_1, \dots, \beta_t)$ and argument list $(v_1, \dots, v_t)$. Then $u = x\alpha + y\beta$. By the induction hypothesis, it follows that $f(x)$ is an F-linear combination with scalar list $(\alpha_1, \dots, \alpha_s)$ and argument list $\big(f(u_1), \dots, f(u_s)\big)$, while $f(y)$ is an F-linear combination with scalar list $(\beta_1, \dots, \beta_t)$ and argument list $\big(f(v_1), \dots, f(v_t)\big)$. Then by the equations (3.20), the image $f(u) = f(x\alpha + y\beta) = f(x)\alpha + f(y)\beta$ is an F-linear combination with scalar list $(\alpha_1\alpha, \dots, \alpha_s\alpha, \beta_1\beta, \dots, \beta_t\beta)$ and argument list $\big(f(u_1), \dots, f(u_s), f(v_1), \dots, f(v_t)\big)$. □

4. Categories of relations

4.1. **Relations between sets.** Over a field with more than one element, the category of linear transformations between finite-dimensional vector spaces is self-dual. In particular, each singleton vector space $\{0\}$ is both initial and terminal. On the other hand, even restricting to finite sets, the category of functions between sets is not self-dual. For example, the initial object is the empty set, while the terminal objects are the singletons. In order to construe sets as objects of a category of vector spaces over the one-element field $\mathsf{GF}(1)$, the appropriate category is the category **Rel** of relations between sets, not the category **Set** of functions between sets.

Thus the object class of **Rel** is the class of sets. For sets X and Y, the morphism set $\mathbf{Rel}(X,Y)$ is the set of relations ρ from X to Y, i.e. the set of subsets ρ of the Cartesian product $X \times Y$ in **Set**. The composition is given by

$$\mathbf{Rel}(X,Y)\times\mathbf{Rel}(Y,Z)\to\mathbf{Rel}(X,Z);(\rho,\sigma)\mapsto\rho\circ\sigma$$

with the *relation product*

$$\rho\circ\sigma=\{(x,z)\in X\times Z\mid\exists\, y\in Y\,.\,(x,y)\in\rho\text{ and }(y,z)\in\sigma\}\,.$$

A function $f\colon X\to Y$ may be identified with its *graph*

$$\{(x,y)\in X\times Y\mid xf=y\}$$

so that the relational product restricts to the composition of functions. Then **Set** is included as a subcategory of **Rel**. In particular, the identity at an object X of **Rel** is the equality relation on X, the graph 1_X of the identity function $1_X\colon X\to X$.

Lemma 4.1. *The disjoint union $X\oplus Y$ of two sets X and Y serves as a biproduct in* **Rel**, *both the product and coproduct of X and Y.*

Proof. The insertions into the biproduct are given by the (graphs of the) usual insertions $\iota_X\colon X\to X\oplus Y$ and $\iota_Y\colon X\to X\oplus Y$ into the disjoint union. Recall the right distributive law $(X\oplus Y)\times Z=(X\times Z)\oplus(Y\times Z)$ in **Set**. Then for relations $\rho\colon X\to Z$ and $\sigma\colon Y\to Z$, the sum $\rho+\sigma\colon X\oplus Y\to Z$ is the disjoint union $\rho\oplus\sigma$ as a subset of $(X\times Z)\oplus(Y\times Z)$. Thus

$$\iota_X\circ(\rho+\sigma)=\rho\quad\text{ and }\quad\iota_Y\circ(\rho+\sigma)=\sigma$$

as required.

The respective projections from the biproduct are the relations

$$\pi_X=\{(x\iota_X,x)\in(X\oplus Y)\times X\mid x\in X\}$$

and

$$\pi_Y=\{(y\iota_X,y)\in(X\oplus Y)\times Y\mid y\in Y\}\,.$$

Recall the left distributive law $Z\times(X\oplus Y)=(Z\times X)\oplus(Z\times Y)$ in **Set**. Then for relations $\rho\colon Z\to X$ and $\sigma\colon Z\to Y$, the product $\rho\times\sigma\colon Z\to X\oplus Y$ is the disjoint union $\rho\oplus\sigma$ as a subset of $(Z\times X)\oplus(Z\times Y)$. Thus

$$(\rho\times\sigma)\circ\pi_X=\rho\quad\text{ and }\quad(\rho\times\sigma)\circ\pi_Y=\sigma$$

as required. □

Lemma 4.2. *The category* **Rel** *has an internal hom functor* **rel** *given by*

$$\mathbf{rel}(Y,Z)=Y\times Z$$

for sets Y,Z.

Proof. Observe that

$$\mathbf{Rel}\big(\mathsf{GF}(1), Y \times Z\big) \cong 2^{Y \times Z} = \mathbf{Rel}(Y, Z)$$

via the natural isomorphism sending a relation $\rho \subseteq \mathsf{GF}(1) \times (Y \times Z)$ to the subset $\{(y, z) \mid \big(0, (y, z)\big) \in \rho\}$ of $Y \times Z$. □

Remark 4.3. Lemma 4.2 may also be justified on the basis that **Rel** is the Kleisli category for the covariant power set endofunctor of **Set**, noting the nature of the underlying set functor for the Kleisli category [14, Th. VI.5.1].

Lemma 4.4. *The Cartesian product $X \otimes Y$ of two sets X and Y serves as a tensor product in* **Rel**, *by virtue of the adjunction*

$$\mathbf{Rel}(X \otimes Y, Z) \cong \mathbf{Rel}(X, \mathbf{rel}(Y, Z)) \tag{4.1}$$

between $Y \mapsto X \otimes Y$ and $Y \mapsto \mathbf{rel}(Y, Z)$.

Proof. Each side of (4.1) is the power set $2^{X \times Y \times Z}$. □

We may summarize as follows.

Theorem 4.5. *The category* **Rel** *supports symmetric monoidal category structures $\big(\mathbf{Rel}, \oplus, \emptyset\big)$ and $\big(\mathbf{Rel}, \otimes, \mathsf{GF}(1)\big)$, with the disjoint union $X \oplus Y$ as the biproduct and the Cartesian product $X \otimes Y$ as the tensor product of sets X and Y.*

For a field F with more that one element, write $\underline{\underline{F}}^{<\omega}$ for the category of linear transformations between finite-dimensional vector spaces over F. Theorem 4.5 may then be viewed against the following.

Theorem 4.6. *The category $\underline{\underline{F}}^{<\omega}$ supports symmetric monoidal category structures $\big(\underline{\underline{F}}^{<\omega}, \oplus, \{0\}\big)$ and $\big(\underline{\underline{F}}^{<\omega}, \otimes, F\big)$.*

In order to unify the notation for fields with one or more elements, we introduce the following definition.

Definition 4.7. The category $\underline{\underline{\mathsf{GF}(1)}}^{<\omega}$ is the full subcategory of **Rel** whose object class is the class of finite sets.

With this notation established, Theorem 4.6 applies equally well for fields F with one or more elements.

4.2. **Linear algebra.** The categories $\underline{\underline{F}}^{<\omega}$ specified in the preceding section provide support for a unified treatment of linear algebra covering fields F with one or more elements. We offer some illustrative fragments. In particular, the following definition provides an answer to [3, Puzzle 1], which asked “In what way is an n-element set like $\mathbb{F}_1^n$?”

Definition 4.8. Let F be a field with one or more elements. For a natural number d, define the reference space

$$F^d = \overbrace{F \oplus F \oplus \ldots \oplus F}^{d \text{ summands}} \tag{4.2}$$

as the d-th direct power of F in the category $\underline{\underline{F}}^{<\omega}$.

With $d = 0$, Definition 4.8 returns the zero object of $\underline{\underline{F}}^{<\omega}$, namely $\{0\}$ for $|F| > 1$ or $\emptyset$ for $|F| = 1$.

Definition 4.9. Let V be a vector space over a field F. Suppose that d is a natural number. Then V is said to have (*finite*) *dimension* d if it is linearly isomorphic to the reference space F^d.

Proposition 4.10. *Let V be a vector space over a field F. Let d be a natural number.*

(a) *If $|F| = 1$, then V has dimension d if and only if $|V| = d$.*
(b) *If $|F| > 1$, then V has dimension d in the sense of Definition 4.9 if and only if it has dimension d in the classical sense* [10, §8].

Proof. (a) By Theorem 3.22(a), the set V has dimension d if and only if, as a set, it is isomorphic to F^d. But by Definition 4.8, $|F^d| = d$.

(b) By Theorem 3.22(b), the space V has dimension d if and only if it is classically isomorphic to the vector space F^d. □

The following definition is introduced to show how the concepts of linear independence and basis may be worked in to the present setting.

Definition 4.11. Let V be a vector space over a field F. Consider a (possibly empty) ordered list $(v_1, \ldots, v_d)$ of vectors from V.

(a) The ordered list is *linearly independent* if the span of $\{v_1, \ldots, v_d\}$ is linearly isomorphic to the reference space F^d.
(b) The ordered list is an *ordered basis* for V if it is linearly independent and spans V.

Now consider a linear transformation $f\colon V \to W$ from a vector space V of dimension m to a vector space W of dimension n. Suppose that V has an ordered basis $(v_1, \ldots, v_m)$ and W has an ordered basis $(w_1, \ldots, w_n)$. We present a unified way to specify the linear transformation $f\colon V \to W$ by its matrix $[f_{ij}]_{m\times n}$ with respect to the ordered bases $(v_1, \ldots, v_m)$ and $(w_1, \ldots, w_n)$. Let the ordered bases correspond to linear isomorphisms $\upsilon\colon V \to F^m$ and $\omega\colon W \to F^n$. Then for $1 \le i \le m$ and $1 \le j \le n$, the diagram

$$\begin{tikzcd}
F^m \arrow[r, "\upsilon^{-1}"] \arrow[d, equal] & V \arrow[r, "f"] & W \arrow[r, "\omega"] & F^n \arrow[d, equal] \\
\bigoplus_{k=1}^m F & F \arrow[l, "\iota_i"'] \arrow[r, dashed, "f_{ij}"'] & F & \bigoplus_{k=1}^n F \arrow[l, "\pi_j"']
\end{tikzcd}$$

in $\underline{\underline{F}}^{<\omega}$ specifies the entries of the matrix as morphisms $f_{ij}\colon F \to F$. When $|F| > 1$, these morphisms are scalar multiplications, and then the matrix entries are usually considered as the corresponding scalars. If $|F| = 1$, the morphisms are relations from F to F. There are only two such relations, namely $\emptyset$ and 1_F. Thus the specification

$$f_{ij} = \begin{cases} 1_F & \text{if } v_i f = w_j; \\ \emptyset & \text{otherwise} \end{cases}$$

describes the matrix directly in this case. In combinatorial terms, we have the incidence matrix of the subset f of $V \times W$. Incidence matrices are usually written with entries 0 and 1, imagined as elements of some nontrivial unital commutative ring or semiring, but in our approach, the entries are just elements of the endomorphism monoid $\{\emptyset, 1_F\}$ of F in $\underline{\underline{F}}^{<\omega}$ or **Rel**.

4.3. **Counting.** For certain counting problems in linear algebra over finite fields $\mathsf{GF}(q)$, the number q is viewed as a parameter. The answers to such counting problems are then formulated in terms of so-called "q-analogs" of ordinary numbers and functions [3, §2], [11], [15, p.6]. Our goal is to show that some well-known counting results of this type carry over seamlessly in our approach to the case $q = 1$.

Definition 4.12. Consider a parameter q.

(a) For a natural number n, the quantity

$$[n]_q = q^{n-1} + q^{n-2} + \ldots + q + 1$$

is called a *q-number*. In particular, $[0]_q$ is the empty sum 0.

(b) For a natural number n, the product

$$[n]_q^! = [n]_q[n-1]_q \ldots [2]_q[1]_q$$

is called a *q-factorial*. In particular, $[0]_q^!$ is the empty product 1.

(c) For natural numbers $k \leq n$, the quotient

$$\binom{n}{k}_q = \frac{[n]_q^!}{[n-k]_q^![k]_q^!}$$

is called a *q-binomial coefficient* or a *Gaussian binomial coefficient.*

The names and notation of Definition 4.12 may be justified as follows.

Lemma 4.13. *Consider a parameter q.*

(a) *For a natural number n, one has $[n]_q = n$ for $q = 1$.*
(b) *For a natural number n, one has $[n]^!_q = n!$ for $q = 1$.*
(c) *For natural numbers $k \leq n$, one has $\binom{n}{k}_q = \frac{n!}{(n-k)!k!} = \binom{n}{k}$ for $q = 1$.*

Our approach to the field with one element thus allows us to formulate the following extensions of well-known results for $q > 1$.

Theorem 4.14. *Within an n-dimensional vector space over a field $\mathsf{GF}(q)$, where $q \geq 1$, the q-binomial coefficient*

$$\binom{n}{k}_q$$

enumerates the k-dimensional vector subspaces. In particular, the number of 1-dimensional subspaces of an n-dimensional space is given by the q-number $[n]_q$.

Now recall that in any vector space, a *flag* is a chain of proper inclusions of subspaces:

$$S_0 \subset S_1 \subset \ldots \subset S_r \,. \tag{4.3}$$

The flag (4.3) is said to have *length* r. Note that the properness of the inclusions implies that for $1 \leq i < j \leq r$, the dimension of S_i is strictly less than the dimension of S_j. In a vector space of dimension r, a flag (4.3) of length r is described as *maximal*.

Theorem 4.15. *Let n be a natural number. Then in a vector space V of dimension n over the field $\mathsf{GF}(q)$, there are $[n]^!_q$ maximal flags.*

Proof. A maximal flag has the form (4.3) with $r = n$. Note that S_0 is just the unique zero-dimensional subspace. It will be shown, by induction on i, that the number of choices for the initial segment $S_0 \subset S_1 \subset \ldots \subset S_i$ of a maximal flag (4.3) of length n is

$$[n]_q \cdot [n-1]_q \cdot \ldots \cdot [n-(i-1)]_q \tag{4.4}$$

for $1 \leq i \leq n$. The desired result follows on noting that (4.4) takes the form $[n]^!_q$ when $i = n$.

For the induction basis $i = 1$ with $q > 1$, there are $q^n - 1$ nonzero vectors that may be chosen to span S_1, and any $q - 1$ of these span the same space S_1. Thus the number of choices for S_1 is $(q^n - 1)/(q - 1) = [n]_q$. Similarly, for $q = 1$, any one of the $n = [n]_1$ elements of V may be chosen as the unique element of S_1. This completes the induction basis.

Now suppose that (4.4) is a correct count for the initial segments of length i, where $1 \leq i < n$. Consider the problem of determining S_{i+1}.

(a) If $q = 1$, any one of the $n - i = [n - i]_q$ elements x of $V \smallsetminus S_i$ may be chosen to build S_{i+1} as $\mathrm{Span}(S_i \cup \{x\}) = S_i \cup \{x\}$, so there are $[n]_q \cdot \ldots \cdot [n - i]_q$ possible initial segments of length $i + 1$.

(b) If $q > 1$, any one of the $q^n - q^i$ elements x of $V \smallsetminus S_i$ may be chosen to build S_{i+1} as $\mathrm{Span}(S_i \cup \{x\})$. In this case, any of the $q^{i+1} - q^i$ elements of $S_{i+1} \smallsetminus S_i$ will work along with S_i to span the same space S_{i+1}. Thus the number of choices for a space S_{i+1} extending the given initial segment is

$$\frac{q^n - q^i}{q^{i+1} - q^i} = \frac{q^{n-i} - 1}{q - 1} = [n - i]_q \,,$$

and again there are $[n]_q \cdot \ldots \cdot [n - i]_q$ possible initial segments of length $i + 1$.

This completes the induction step. □

5. Conclusion

By use of quasigroup features, we have augmented the definition of a field to include the field of order one. By use of linear hyperquasigroups, we have broadened the concept of a linear combination to construe sets as vector spaces over the field with one element. We have then shown that the category of relations is the appropriate category for extending linear algebra to cover these vector spaces over the field with one element. The application of linear-algebraic counting formulae involving q-numbers, q-factorials, and q-binomial coefficients is then extended to the case where $q = 1$.

References

[1] L.A. Bokut, Y. Chen and Q. Mo, Gröbner-Shirshov bases and embeddings of algebras, *Internat. J. Algebra Comput.* **20** (2010), 875–900.

[2] J.M. Borger, *Λ-rings and the field with one element*, `arxiv.org/abs/0906.3146`, 2009.

[3] H. Cohn, Projective geometry over $\mathbf{F}_1$ and the Gaussian binomial coefficients, *Amer. Math. Monthly* **111** (2004), 487–495.

[4] A. Connes and C. Consani, On the notion of geometry over $\mathbb{F}_1$, *J. Algebraic Geom.* **20** (2011), 525-557.

[5] S. Doro, Simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **83** (1978), 377–392.

[6] N. Durov, *New Approach to Arakelov Geometry*, `arxiv.org/abs/0704.2030v1`, 2007.

[7] T. Evans, Homomorphisms of non-associative systems, *J. London Math. Soc.* **24** (1949), 254–260.

[8] T. Evans, Embedding theorems for multiplicative systems and projective geometries, *Proc. Amer. Math. Soc.* **3** (1952), 614–620.

[9] T. Evans, Varieties of loops and quasigroups, pp. 1–26 in *Quasigroups and Loops: Theory and Applications* (O. Chein, H.O. Pflugfelder and J.D.H. Smith, eds.), Heldermann, Berlin, 1990.

[10] P.R. Halmos, *Finite-Dimensional Vector Spaces* (2nd. edition), Van Nostrand, Princeton, NJ, 1958.

[11] V. Kac and P. Cheung, *Quantum Calculus*, Springer, New York, NY, 2002.

[12] M. Kapranov and A. Smirnov, *Cohomology determinants and reciprocity laws: number field case*, Preprint series, Institut für experimentelle Mathematik, Essen, 1995. http://www.neverendingbooks.org/DATA/KapranovSmirnov.pdf

[13] O. Lorscheid, *Algebraic groups over the field with one element*, arxiv.org/abs/0907.3824v1, 2009.

[14] S. Mac Lane, *Categories for the Working Mathematician*, Springer, New York, NY, 1971.

[15] S. Majid, *A Quantum Groups Primer*, Cambridge University Press, Cambridge, 2002.

[16] Yu.I. Manin, (1995), Lectures on zeta functions and motives (according to Deninger and Kurokawa), *Astérisque* **228** 121-163.

[17] A.I. Malcev, On a representation of nonassociative rings (Russian), *Uspekhi Mat. Nauk N.S.* **7** (1952), 181–185.

[18] J.D.H. Smith, Axiomatization of quasigroups, *Discuss. Math. Gen. Alg. and Appl.* **27** (2007), 21–33.

[19] J.D.H. Smith, Evans' normal form theorem revisited, *Internat. J. Algebra Comput.* **17** (2007), 1577–1592.

[20] J.D.H. Smith, Ternary quasigroups and the modular group, *Comment. Math. Univ. Carol.* **49** (2008), 309–317.

[21] J.D.H. Smith, Groups, triality, and hyperquasigroups, *J. Pure Appl. Algebra* **216** (2012), 811-825.

[22] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[23] C. Soulé, Les varietés sur le corps à un élément, *Mosc. Math. J.* **4** (2004), 217–244.

[24] J. Tits, Sur les analogues algébriques des groupes semi-simples complexes, pp.261-289 in *Colloque d'Algèbre Supérieure*, Ceuterick, Louvain, 1957.

Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.

E-mail address: jdhsmith@iastate.edu

URL: http://orion.math.iastate.edu/jdhsmith/