DE GRUYTER
OPEN

DOI 10.1515/tmj-2015-0002

The field $\mathbb{F}_8$ as a Boolean manifold

René Guitart

IMJ-PRG Université Paris Diderot, Bâtiment Sophie Germain, 75013 Paris, France
E-mail: rene.guitart@orange.fr

For my friend Marco Grandis, on the occasion of his 70th birthday

Abstract

In a previous paper ("Hexagonal Logic of the Field $\mathbb{F}_8$ as a Boolean Logic with Three Involutive Modalities", in *The road to Universal Logic*), we proved that elements of $\mathbb{P}(8)$, i.e. functions of all finite arities on the Galois field $\mathbb{F}_8$, are compositions of logical functions of a given Boolean structure, plus three geometrical cross product operations. Here we prove that $\mathbb{P}(8)$ admits a purely logical presentation, as a *Boolean manifold*, generated by a diagram of 4 Boolean systems of logical operations on $\mathbb{F}_8$. In order to obtain this result we provide various systems of parameters of the set of unordered bases on $\mathbb{F}_2^3$, and consequently parametrical polynomial expressions for the corresponding conjunctions, which in fact are enough to characterize these unordered bases (and the corresponding Boolean structures).

2010 Mathematics Subject Classification. **03B50**. 03G05, 06Exx, 06E25, 06E30, 11Txx.
Keywords. Boolean algebra, many-valued logics, finite fields.

1 Introduction

Informally this paper could be understood as a 'functional' reflexion on the cube, i.e. in fact on $\{0,1\}^3 = \underline{2}^3 = \underline{8}$, as an attempt to construct all the internal functions of any arities on $\underline{8}$ from ordinary Boolean logical functions combined in a geometrical way; this will exhibit $\underline{2}^3 = \underline{8}$ as a so called *Boolean manifold*. The point is to make this perspective completely rigorous.

1.1 Preamble: Notions of Boolean manifold and of Boolean shape of q-logics

In this first introductive sub-section, we precise the conducting ideas of *Boolean manifold* and of *Boolean shape* of a theory, at the root of developments expressed in the second sub-section 1.2.

We begin with explaining the notion of a *Boolean atlas* for a q-logic and of the Boolean shape of q understood as the shape of such an atlas (if it exists) for the canonical q-logic on $\underline{q}$. Then the problem is specified in the case of $q = 2^n$, indeed in the case $q = 4$.

1.1.1 q-logic

Definition 1.1. 1 — Given a set Q, we define the *logical theory generated by* Q, as being the full subcategory $\mathrm{G}(Q)$ of the category Set of sets and functions *generated by* Q and its finite powers Q^k; as a case of a Lawvere theory, this category equipped with its cartesian product is denoted by $\mathbb{G}(Q)$.
2 — An algebra in Set of this theory $\mathbb{G}(Q)$, i.e. a functor

$$M : \mathbb{G}(Q) \to \mathrm{Set}$$

Tbilisi Mathematical Journal 8(1) (2015), pp. 31–62.
Tbilisi Centre for Mathematical Sciences.
Received by the editors: 21 October 2014.
Accepted for publication: 21 October 2014.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

preserving the powers, i.e. such that for every k, $M(Q^k) = M(Q)^k$, is named a *Q-logic*. Roughly it is a set $E = M(Q)$ equipped with an 'action' of $\mathbb{G}(Q)$.
3 — The 'fundamental example' of a Q-logic corresponds to the canonical inclusion

$$J_Q : \mathbb{G}(Q) \hookrightarrow \mathrm{Set},$$

and it is the *'canonical' Q-logic on the set Q*.
4 — A Q-logic could also be introduced as a $\mathbb{P}(Q)$-*module*, i.e. a set E with an 'action' of the Post-Malcev iterative algebra $\mathbb{P}(Q) = \cup_{k\in\mathbb{N}} Q^{(Q^k)}$, i.e., with $M(Q) = E$, and $\mathbb{P}(E) = \cup_{k\in\mathbb{N}} E^{(E^k)}$, a morphism of Post-Malcev algebras

$$\mu_M : \mathbb{P}(Q) \to \mathbb{P}(E).$$

Especially for the canonical Q-logic on Q we have

$$\mu_{J_Q} = \mathrm{Id}_{\mathbb{P}(Q)} : \mathbb{P}(Q) \to \mathbb{P}(Q).$$

5 — Given an integer q and a set $Q = \underline{q} = \{0, 1, 2, \ldots, n-1\}$ with q elements, then $\mathbb{G}(Q) = \mathbb{G}(\underline{q})$ is simply denoted by $\mathbb{G}(q)$, and $\mathbb{P}(\underline{q})$ by $\mathbb{P}(q)$, and a Q-logic is named a *q-logic*.

1.1.2 Boolean chart, Boolean manifold, Boolean shape: case $q = 2^n$

Proposition 1.2. The different axiomatics of a Boolean algebra are just different generators systems of $\mathbb{G}(2)$ — or equivalently of $\mathbb{P}(2)$ — and so a 2-logic is exactly a Boolean algebra.

Proposition 1.3. Each morphism of theories

$$K : \mathbb{G}(2) \to \mathbb{G}(q),$$

with $K(\underline{2}^k) = \underline{q}^k$ — or the associated $\mu_K : \mathbb{P}(2) \to \mathbb{P}(q)$ — determines a Boolean structure M_K on any set E equipped with a q-logic M; this M_K is given by MK as well as by $\mu_M\mu_K$. So MK is seen as a *Boolean chart* on E.

The next Definition 1.4 is almost the same but a little different from the notion of a *Logical manifold* introduced in [1].

Definition 1.4. A q-logic M on a set E — given by a map $\mu_M : \mathbb{G}(q) \to \mathbb{G}(E)$ — is a *Boolean manifold* if there exists a family $\big(K_i : \mathbb{G}(2) \to \mathbb{G}(q)\big)_{i\in I}$ of morphisms such that from the family $(M_{K_i})_{i\in I}$ of Boolean structures, we can recover M itself, i.e.

$$\mathrm{Im}\,\mu_M = \mathrm{Comp}\big(\cup_{i\in I} \mathrm{Im}\,\mu_{MK_i}\big),$$

in other terms each function of $\mathbb{P}(E)$ of the form $\mu_M(f)$, with f in $\mathbb{P}(q)$, is a composition of "Boolean" functions of the form $\mu_{MJ_i}(b)$, with $b \in \mathbb{P}(2)$.
If μ_M is surjective — as it is the case for the 'canonical' q-logic on the set $\underline{q}$ — the family of morphisms $\mu_M\mu_{K_i} : \mathbb{P}(2) \to \mathbb{P}(E)$ is said *composition surjective*, and is named a *Boolean atlas* on M.

Basic Question : Given an integer q, is it true that the canonical q-logic on $\underline{q}$ is a Boolean manifold, i.e. admits a Boolean atlas $\big(\mu_{K_i} : \mathbb{P}(2) \to \mathbb{P}(q)\big)_{i\in I}$? Furthermore, if this is true, what is the minimal cardinal of such a Boolean atlas, how is its geometry, what are its symmetries ? To speak roughly, what is the *Boolean shape* of q ?

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Remark 1.5. In fact the categorical setting of *shape theory* would give a formal definition of the Boolean shape of a q-logic, or of $\mathbb{G}(q)$, or even of any Lawvere theory $\mathbb{T}$ as follows. The Boolean shape of a theory $\mathbb{T}$ is the category with objects the morphisms $K : \mathbb{G}(2) \to \mathbb{T}$, and with morphisms from K to K' an endomorphism θ of $\mathbb{G}(2)$ such that $T'\theta = T$. Then the 'Boolean component' of $\mathbb{T}$ is $\mathbb{T}_{\text{Boole}} = \lim_\theta \mathbb{G}(2)$, and $\mathbb{T}$ is a Boolean manifold if the canonical map $\mathbb{T}_{\text{Boole}} \to \mathbb{T}$ is an epimorphism.

Proposition 1.6. If $q = 2^n$, then the canonical q-logic on the set $\underline{2}^n$ is a Boolean manifold, i.e. $\mathbb{P}(2^n)$ is generated by the union of copies of $\mathbb{P}(2)$. Moreover if n is even (resp. odd) we can find a Boolean atlas with 3 (resp. 4) elements.

Proof. See [2, Theorem 1, Theorem 7]. The crucial point is that $\underline{2}^n$ is a finite field of characteristic 2, and is equipped with a Frobenius map $x \mapsto x^2$. Q.E.D.

Remark 1.7. Two Boolean structures $\mu_K, \mu_{K'} : \mathbb{P}(2) \to \mathbb{P}(\underline{2}^n)$ are dual if $\mu_{K'} = \mu_K(-)^{\text{op}}$, where $(-)^{\text{op}} : \mathbb{P}(2) \to \mathbb{P}(2)$ is the duality induced by the negation $\nu : \{0,1\} \to \{0,1\} : 0 \mapsto 1, 1 \mapsto 0$. We have to notice that in this case the images of μ_K and $\mu_{K'}$ are the same Post-Malcev sub-algebra of $\mathbb{P}(E)$. So the number of sub-algebras of $\mathbb{P}(\underline{2}^n)$ obtained by copying $\mathbb{P}(2)$ is half the number of Boolean structures on $\underline{2}^n$.

Proposition 1.8. If $q = 2^2 = 4$, then the canonical 4-logic on the set $\underline{2}^n$ is a Boolean manifold, i.e. $\mathbb{P}(4)$ is generated by composition of 3 copies of $\mathbb{P}(2)$.

Proof. It is a special case of 1.6; but an explicit and detailed description of this union, as a 'Borromean object' in the category of Post-Malcev algebras, is given in [4, Proposition 9.5.]: 3 copies of $\mathbb{P}(2)$ are enough, and could be chosen in a 'symmetrical position'. Q.E.D.

Remark 1.9. We know that on a set $\underline{2}^n$ there is exactly one structure of field, up to isomorphisms, and, similarly one structure of Boolean algebra, up to isomorphisms; hence the question of the relation between these fields and these Boolean algebras. Clearly, if we start with a field 2^n, and if we choose a basis over $\mathbb{F}_2$, then a component-wise calculus provides a Boolean structure. Conversely of course if we start with a Boolean algebra 2^n, we cannot recover the multiplication of the field 2^n by compositions of its logical functions; but if we consider the simultaneous data of *several* Boolean structures (isomorphic but different), then we can recover the field multiplication — this is what Proposition 1.6 says. Whence a justification of the notion of a Boolean manifold.

1.2 Purpose and results in the case $q = 8$

Now, in this second introductive sub-section, we explain the results obtained here when $q = 8$.

The purpose of this paper is to discribe precisely what is the *Boolean shape* of the 8-valued logic [for this notion of *Boolean shape* see section 1.1], how it is generated, what kind of symmetries it has, what natural parameters can exhibit these symmetries.

In fact 8 is very special, it is 2^3, the smallest 3-dim space, and there we have a very rich system of interactions between arithmetic (finite field), geometry (cross product, mixed product, linear maps), logic (Boolean structures). On the way toward the explanation of the Boolean shape of the Boolean manifold 8 we have to use these interactions, and to show how each one of these 3 domains could be expressed with respect to the 2 others.

In section 2 we recall notations and objects related to $\mathbb{F}_8$ and $\mathbb{P}(8)$, and especially the field structure on $\mathbb{F}_8$, the special description of the linear group $\text{GL}_3(\mathbb{F}_2)$ given in [3], and the result of

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

[5]: the Post-Malcev full iterative algebra $\mathbb{P}(8)$ of all functions of all finite arities on a set $\underline{8}$ with 8 elements, e.g. on the Galois field $\mathbb{F}_8$, is generated in a logico-geometrical way, by a Boolean logic plus three cross product operations.

One essential tool is the description of the 168 bases of $\mathbb{F}_8$ as permutations of 28 bases which are "multiples" of the 4 auto-dual bases (Proposition 3.11), adapted from [3] and [5], according to the results on $\mathrm{GL}_2(\mathbb{F}_2)$ recalled in section 2. We give two tables, in Propositions 3.13 and 3.20.

In concrete terms the work is realized by introducing convenient parameters for unordered bases and for conjunctions. Actually our METHOD is to try to obtain better and better parametrizations of bases, and ultimately an easy parametric formula for conjunctions; then such a formula will permit to produce tables and combinations of various conjunctions, and so to try to generate any function, and especially to generate the law of the field.

In the case of $\mathbb{F}_4$, each basis is characterized by its 'true' t; but now in the case of $\mathbb{F}_8$ this data t is not enough, and we have to determine supplementary parameters, if possible with a logical meaning. it will be the case with our parameters a and c.

In sections 3 and 4 we construct several parametrizations of the set of Boolean logics on $\underline{8}$, or more precisely of the Boolean logics for which false is 0 and the symmetrical difference is $+$; or, equivalently of the set of the 28 unordered bases of $\mathbb{F}_8$ over $\mathbb{F}_2$.

Mainly we introduce two special systems of parameters for a basis ε: one is the system of independent parameters (t, a) consisting of the 'true' t and the 'association' a (Proposition 3.12); another is the system (t, c) of two dependent parameters 'true' t and 'co-true' c — which is the 'true' of the basis ε^* which is dual of ε — (Proposition 3.18). These parameters determine ε except for the order of its terms.

Furthermore, given a basis ε, the corresponding conjunction is a polynomial, with *polynomial coefficients* $\varepsilon_6, \varepsilon_5, \varepsilon_3$, as in Propositions 4.4 and 4.5, and we obtain the relations between these coefficients (Proposition 4.13), and their expression with respect to t and a, or to t and c (Proposition 4.11); in fact these coefficients could be replaced by coefficients $d_6 = \varepsilon_6 + 1, d_5 = \varepsilon_5, d_3 = \varepsilon_3 + 1$ (Definition 4.19), which are named *differential coefficients* because they furnish the difference between the conjunction $\wedge_\varepsilon$ associated to ε and the canonical conjunction $\wedge = \wedge_\kappa$ associated to the canonical basis κ (Proposition 4.20). We compute these differentials with respect to t and a, and with respect to t and c. These differentials are also directly related to some *canonical parameters* ρ, σ, ι (Definition 4.14).

So explicit parametric formulas are possible for conjunctions (Propositions 4.10, 4.11, 5.5), as, with $u \times v = \big(uv(u+v)\big)^2$:

$$u \wedge_\varepsilon v = u \wedge v + (c^5 + 1)(u \times v) + (c^5 t + t^3)(u \times v)^2 + (c^5 t^3 + 1)(u \times v)^4,$$

and complete tables are furnished (Propositions 5.2 and 5.3).

Then combinations of the logical functions of the Boolean logics on 8 become easy to do, and the description of a Boolean atlas is deduced (Proposition 6.8), with 5 functions — namely the 2 functions $\wedge = \wedge_\kappa, \neg = \neg_\kappa$, and a circularly symmetrical set of 3 functions $\wedge_r, \wedge_s, \wedge_i$. Rather than r, s, i we can use other systems, as $\wedge_A, \wedge_B, \wedge_C$ or $\wedge_{A^*}, \wedge_{B^*}, \wedge_{C^*}$. So, in several ways, $\mathbb{P}(8)$ is generated by composition of 4 copies of $\mathbb{P}(2)$: it is a Boolean manifold.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

2 The field $\mathbb{F}_8$, the Boolean algebra $\mathbb{F}_2^3$, the simple group $\mathrm{GL}_3(\mathbb{F}_2)$, and the Post-Malcev algebra $\mathbb{P}(8)$

We recall notations and results from previous papers [2], [3], [4] and [5]; thus we explain our starting point, the geometrico-logical construction of $\mathbb{P}(8)$.

2.1 The Galois field $\mathbb{F}_8$ and the Boolean algebra $\mathbb{F}_2^3$

Definition 2.1. Let $\mathbb{F}_2 = \{0, 1\}$ be the field with two elements. The field $\mathbb{F}_8$ with 8 elements is the set $\{0, 1, R, S, I, R', S', I'\}$ equipped with the two operations . and + given by the tables

.	R	S	I	R'	S'	I'
R	S	I'	S'	1	R'	I
S	I'	I	R'	R	1	S'
I	S'	R'	R	I'	S	1
R'	1	R	I'	S'	I	S
S'	R'	1	S	I	I'	R
I'	I	S'	1	S	R	R'

+	R	S	I	R'	S'	I'	1
R	0	R'	I'	S	R'	I	S'
S	R'	0	S'	R	I	1	I'
I	I'	S'	0	1	S	R	R'
R'	S	R	1	0	I'	S'	I
S'	R'	I	S	I'	0	R'	R
I'	I	1	R	S'	R'	0	S
1	S'	I'	R'	I	R	S	0

The elements R, S, I are the roots of $X^3 + X^2 + 1 = 0$, with inverses given by

$$R^{-1} = R', S^{-1} = S', I^{-1} = I',$$

which are the roots of $X^3 + X + 1 = 0$, and so

$$\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X^2 + 1) \simeq \mathbb{F}_2[X]/(X^3 + X + 1).$$

Remark 2.2. For litteral computations we use the following formulas:

$$R' = R^{-1} = I + 1 = SI = R + S;$$
$$S' = S^{-1} = R + 1 = IR = S + I;$$
$$I' = I^{-1} = S + 1 = RS = I + R.$$
$$R = R, R^2 = S, R^3 = I', R^4 = I, R^5 = S', R^6 = R';$$
$$S = S, S^2 = I, S^3 = R', S^4 = R, S^5 = I', S^6 = S';$$
$$I = I, I^2 = R, I^3 = S', I^4 = S, I^5 = R', I^6 = I'.$$

Also we use the facts that for all u, $u + u = 0$, $u^8 = u$, and if $u \neq 0$ then $u^7 = 1$, and $u^{-1} = u^6$. For any u and v, $uv = vu$, $u + v = v + u$, and $u = v^2$ is equivalent to $v = u^4$, $u = v^3$ is equivalent to $v = u^5$, $u = v^6$ is equivalent to $v = u^6$.

Definition 2.3. The field $\mathbb{F}_8$ is a $\mathbb{F}_2$-linear space, isomorphic to $\mathbb{F}_2^3$, with a *canonical* basis given by $\kappa = (R, S, I)$ (the only strictly auto-normal basis).

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Furthermore we need two $\mathbb{F}_2$-linear maps, the Frobenius *squaring* $(-)^2$, and the *trace* tr, defined by

$$R^2 = S, \quad S^2 = I, \quad I^2 = R; \quad \mathrm{tr}(R) = \mathrm{tr}(S) = \mathrm{tr}(I) = 1;$$

So we have

$$\mathrm{tr}(w) = w + w^2 + w^4.$$

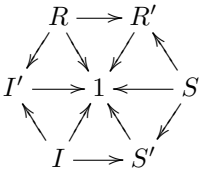
Definition 2.4. The *canonical* Boolean logic $(\wedge, \neg)$ on $\mathbb{F}_8$ is associated to the basis κ: if $u = xR + yS + zI$ and $u' = x'R + y'S + z'I$, then we define $\wedge_\kappa := \wedge, \neg_\kappa := \neg$, with

$$u \wedge u' = (xx')R + (yy')S + (zz')I, \quad \neg u = (x+1)R + (y+1)S + (z+1)I.$$

In particular

$$\neg R = S', \quad \neg S = I', \quad \neg I = R',$$

We draw $\mathbb{F}_8 \backslash \{0\}$ as a hexagon of 'inclusions':



We recover

$$u + u' = (u \wedge \neg u') \vee (\neg u \wedge u').$$

2.2 The Klein group G_{168}

Definition 2.5. The group $\mathrm{GL}_3(\mathbb{F}_2)$ is the group of bijective $\mathbb{F}_2$-linear maps $\mathbb{F}_8 \to \mathbb{F}_8$; it is the only simple group G_{168} with cardinal 168. This G_{168} is also realizable as $\mathrm{PSL}_2(\mathbb{F}_7)$.
We describe $\mathrm{GL}_3(\mathbb{F}_2)$ by matrices relative to the canonical basis $\kappa = (R, S, I)$.
If $u \in \mathbb{F}_8$, $u = xR + yS + zI$, with $x, y, z \in \mathbb{F}_2$, then $\mathrm{Coord}_\kappa(u) := \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ is also denoted $[u]_\kappa$. Each $M \in \mathrm{GL}_3(\mathbb{F}_2)$ is determined by the basis $\varepsilon = (e_1, e_2, e_3)$ such that

$$M = [\mathrm{Coord}_\kappa(e_1) | \mathrm{Coord}_\kappa(e_2) | \mathrm{Coord}_\kappa(e_3)],$$

i.e. the columns of M are the coordinates of e_1, e_2, e_3 relative to κ. Also we write $M = \mathrm{Mat}_\kappa(e_1, e_2, e_3) = \mathrm{Mat}_\kappa(\varepsilon) = [M_\varepsilon]_\kappa = M_\varepsilon$.
By abuse of notations, ε will be assimilated to M, briefly we write $\varepsilon = M$. For example we write $(R', I', 1) = r$.

As usual the identity is denoted by I_3 (different from I above and in notations below). We have

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (-)^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad (-)^4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

$$\mathrm{tr}(-) := I_3 + (-)^2 + (-)^4 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

NOTATIONS — We introduce the following elements of $\mathrm{GL}_3(\mathbb{F}_2)$:

$$r = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad s = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad i = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

$$r^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad s^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad i^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$R = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad I = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$R^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad S^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad I^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Proposition 2.6. The group $\mathrm{GL}_3(\mathbb{F}_2)$ is generated by r, s, i, as well as by r^{-1}, s^{-1}, i^{-1}, as well as by A, B, C; and of course also by the systems of transposes $r^{\mathrm{T}}, s^{\mathrm{T}}, i^{\mathrm{T}}$, $r^{-1^{\mathrm{T}}}, s^{-1^{\mathrm{T}}}, i^{-1^{\mathrm{T}}}$ or $A^{\mathrm{T}}, B^{\mathrm{T}}, C^{\mathrm{T}}$. The center of $\mathrm{GL}_3(\mathbb{F}_2)$ is $\{I_3, R, S, I, R^{-1}, S^{-1}, I^{-1}\}$.

Proof. It is a result from [2] and [3]. In particular we use the fact that the transpositions of r, s, i are given in $\mathrm{GL}_3(\mathbb{F}_2)$ by:

$$r^{\mathrm{T}} = rir^{-1}, \quad s^{\mathrm{T}} = srs^{-1}, \quad i^{\mathrm{T}} = isi^{-1}.$$

We recover the elements R, S, I of the field $\mathbb{F}_8$ in the group $\mathrm{GL}_3(\mathbb{F}_2)$ by

$$R = ir^2, \quad S = rs^2, \quad I = si^2,$$

Also we can exchange r, s, i and A, B, C by:

$$r = ACB, \quad s = BAC, \quad i = CBA,$$

$$A^{\mathrm{T}} = ir, \quad B^{\mathrm{T}} = rs, \quad C^{\mathrm{T}} = si,$$

with $A^{\mathrm{T}}, B^{\mathrm{T}}, C^{\mathrm{T}}$ the transposed matrices of A, B, C, or

$$A = rir^{-1}isi^{-1}, \quad B = srs^{-1}rir^{-1}, \quad C = isi^{-1}srs^{-1}.$$

Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

2.3 Matrices and canonical logical connectors as polynomials

In order to compute with $\mathbb{F}_2$-linear maps and non-linear maps inside the Post-Malcev algebra, we need the *polynomial representation* of matrices with coefficients in $\mathbb{F}_2$ or representations of $\mathbb{F}_2$-linear maps, and their inverses; we need also the calculus with matrices with coefficients in $\mathbb{F}_8$, as in Proposition 2.7.

Proposition 2.7. 1 — Each $\mathbb{F}_2$-linear map $f = \mathbb{F}_8 \to \mathbb{F}_8$, determined by $f(R) = e_1, f(S) = e_2, f(I) = e_3$, and so given by the matrix with coefficients in $\mathbb{F}_2$

$$M_\varepsilon = [\mathrm{Coord}_\kappa(e_1)|\mathrm{Coord}_\kappa(e_2)|\mathrm{Coord}_\kappa(e_3)],$$

is also given by a unique expression

$$f(u) = au^4 + bu^2 + cu,$$

with (using matrices with coefficients in $\mathbb{F}_8$):

$$\begin{bmatrix} c \\ b \\ a \end{bmatrix} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}.$$

The matrix $\mathrm{C}_{RSI} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix}$ will be used frequently in this paper. It will be named the *canonical circular involution*. We have $\mathrm{C}_{RSI}^2 = I_3$.
2 — The map f is invertible if and only if

$$\Delta(f) := a^7 + b^7 + c^7 + abc(a^3b + b^3c + c^3a) \neq 0,$$

and then $f^{-1}(v) = lv^4 + mv^2 + nv$, with

$$l = \frac{b^3 + c^2a}{\Delta(f)}; \quad m = \frac{a^5 + bc^4}{\Delta(f)}; \quad n = \frac{c^6 + a^4b^2}{\Delta(f)}.$$

Proof. See [5, Prop. 3.10-12] Q.E.D.

If we want to mix $\mathbb{F}_2$-linear maps and logic, we have just to express everything as polynomials. For that we have, concerning the *canonical* logic (associated to the canonical basis κ):

Proposition 2.8.

$$u \wedge u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2, \quad \neg u = u + 1$$

$$u \vee u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2 + u + u',$$

$$u \Rightarrow u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2 + u' + 1.$$

Proof. See [5, Prop. 4.8] Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Convention on notations — As $\mathbb{F}_8$ is a finite field, an arbitrary function $f : \mathbb{F}_8 \to \mathbb{F}_8$ could be represented by a polynomial P with coefficients in $\mathbb{F}_8$, and in particular it is true for linear functions. But a $\mathbb{F}_2$-linear f is also representable by matrices M relative to the canonical basis κ (cf. 2.3), with coefficients in $\mathbb{F}_2$, i.e. elements of $\mathrm{M}_3(\mathbb{F}_2)$. If M is a matrix of f and P a polynomial of the same f, we introduce $P_f = P = \underline{M}$, $M_f = M = \hat{P}$, in such a way that $\underline{NM}$ is the product of polynomial QP, whereas $\hat{Q}\hat{P}$ is the composition of matrices NM. For example we have $\underline{r}(u) = R^{-1}u^4 + u^2 + I^{-1}u$, $\underline{A}(u) = R^{-1}u^4 + Iu^2 + Su$, or (cf. 2.10) $\underline{R^\times}(u) = Su^4 + Iu^2$.
Use of $\mathrm{M}_3(\mathbb{F}_8)$ —We mention that not only we compute in $\mathrm{M}_3(\mathbb{F}_2)$, but we also use notations and computations in $\mathrm{M}_3(\mathbb{F}_8)$, considering $\mathbb{F}_2 \subset \mathbb{F}_8$, $\mathbb{F}_2^3 \subset \mathbb{F}_8^3$, $\mathrm{M}_3(\mathbb{F}_2) \subset \mathrm{M}_3(\mathbb{F}_8)$. It is the case in Proposition 2.7, Definition 3.4, Proposition 3.7, Definition 4.1, Propositions 4.6, 4.7, 4.15, 4.16, 4.18, Definition 4.19, Propositions 6.6, 6.7. In such computations a $u \in \mathbb{F}_8$ could be represented by its "Squaring vector" $[u]_{\mathrm{sq}} \in \mathbb{F}_8^3$ (see Definition 3.4), as well as by its coordinates $[u]_\varepsilon$ with respect to a basis ε. A basis $\varepsilon = (e_1, e_2, e_3)$ of $\mathbb{F}_8$ over $\mathbb{F}_2$ could be represented by a matrix M_ε (Definition 2.5), or by a vector $\vec{\varepsilon}$ (in the proof of Proposition 3.13) or by a diagonal matrix Δ_ε (Definition 4.1).

2.4 The Post-Malcev composition algebra

Definition 2.9. $\mathbb{P}(8)$, the Post-Malcev full iterative algebra ([9], [6]) of all functions $f : \mathbb{F}_8^k \to \mathbb{F}_8$ of all arities k on $\mathbb{F}_8$ is

$$\mathbb{P}(8) = \mathbb{P}(\mathbb{F}_8) = \cup_{k\in\mathbb{N}}\mathrm{Hom}_{\mathrm{Set}}({\mathbb{F}_8}^k, \mathbb{F}_8) = \cup_{k\in\mathbb{N}}{\mathbb{F}_8}^{({\mathbb{F}_8}^k)}.$$

Proposition 2.10. The algebra $\mathbb{P}(8)$ is generated by the canonical logic, i.e. $\wedge$ and $\neg$ (and consequently $+$), plus the squaring $(-)^2$ in the field $\mathbb{F}_8$, plus r, s, i.
It is also generated by the canonical logic, i.e. $\wedge$ and $\neg$, plus A, B, C.
And finally it is generated by the canonical logic, i.e. $\wedge$ and $\neg$, plus the linear *non-invertible* maps

$$R^\times = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad S^\times = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad I^\times = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Proof. It is a result from [5]. Q.E.D.

Remark 2.11. The logico-geometrical structure of $\mathbb{F}_8$ is to be understood as an analysis of $\mathbb{P}(\mathbb{F}_8) = \mathbb{P}(8)$. So $\mathbb{P}(8)$ appears as an algebra generated, over $\mathbb{F}_8$, by crossing two 'pure' aspects: classic logic and vector geometry, both associated to the basis $\kappa = (R, S, I)$, which together are enough to generate any function in $\mathbb{P}(8)$.
From now on, our objective will be to replace the linear geometrical operations given by $G_{168} = \mathrm{GL}_3(\mathbb{F}_2)$ — and especially the three operations $R^\times, S^\times, I^\times$ used in Proposition 2.10 — by Boolean operations, associated to κ *and* to other different bases.

3 Duality, coordinates, parameters for unordered bases in $\mathbb{F}_8$

Let us notice that if $\varepsilon = (e_1, e_2, e_3)$ is a basis (actually an ordered basis), the corresponding *unordered basis* — or the basis except for the order of its terms — is $\{e_1, e_2, e_3\}$. By abuse of notation this unorderd basis is again denoted by ε. There are 168 bases, and 28 unordered bases.

We introduce computations with *dual* bases and coordinates, in relation with polynomial calculus, using matrices thanks to the order of terms in an ordered basis. We describe two independent

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

parameters t and a named 'true' and 'association', for the presentation of any unordered basis ε. Furthermore we do present 28 bases, representing the 28 unordered bases, by their parametrization with 'true' t and 'co-true' c. With these parameters the duality at the level of unordered bases is simply the exchange of t and c.

The reader is invited to observe the very active part played in our computations and derivations of our parameters by two tools which are on the one hand the field operation and the Frobenius map, and on the other hand the trace (arithmetic), the scalar product and the cross product, the duality (geometry): roughly speaking we can say that we produce the logic from a combination of arithmetic and geometry.

3.1 Bases, dual bases, and calculus of coordinates

Definition 3.1. Given $u = xR + yS + zI$ and $u' = x'R + y'S + z'I$, with $x, y, z, x', y', z' \in \mathbb{F}_2$, the cross product is $\times_\kappa := \times$ with

$$u \times u' = (yz' + zy')R + (zx' + xz')S + (xy' + yx')I,$$

and the scalar product is $< , >_\kappa = < , >$ with

$$< u, u' >= xx' + yy' + zz'.$$

Proposition 3.2. With the operations of the field $\mathbb{F}_8$ we have:

$$u \times u' = (uu'(u + u'))^2, \quad < u, u' >= uu' + (uu')^2 + (uu')^4 = \mathrm{tr}(uu') = \mathrm{tr}(u \wedge u');$$

the mixed product $[u, u', u''] :=< u \times u', u'' >=< u, u' \times u'' >$ is given by

$$[u, u', u''] = \begin{vmatrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \end{vmatrix} = \begin{vmatrix} u & u' & u'' \\ u^2 & u'^2 & u''^2 \\ u^4 & u'^4 & u''^4 \end{vmatrix} \in \{0, 1\}.$$

Furthermore we have the double cross product formula:

$$u \times (u' \times u'') =< u, u'' > u' + < u, u' > u''.$$

Proof. The three formulas come from [5, Propositions 4.3, 4.10, 4.4]). In fact the first formula is true because $u \times u'$ and $(uu'(u + u'))^2$ are bilinear, and are equal when u and u' take the values R, S, I.
For the mixed product we have

$$[u, u', u''] =< u, u' \times u'' >= \mathrm{tr}(u(u' \times u'')) = \mathrm{tr}(u(u'u''(u' + u''))^2),$$

and this is the value of the second determinant. But also we know that $[u, u', u'']$ is the first determinant, and consequently in $\mathbb{F}_2$.
The double cross product formula could be verified directly, with Definition 3.1. Q.E.D.

Proposition 3.3. A data $\varepsilon = (e_1, e_2, e_3)$ is a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$ if and only if

$$e_1e_2e_3(e_1 + e_2)(e_2 + e_3)(e_3 + e_1)(e_1 + e_2 + e_3) = 1.$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proof. It is in [5, Propositions 4.1 et 4.3-4]. Here it results from Proposition 3.2, computing $[e_1, e_2, e_3]$, which is equal to the first member of the proposed identity, and so its value is in $\mathbb{F}_2$. If the first member is not 0 then we have a basis, because then no linear combination of e_1, e_2 and e_3 is 0; then it must be 1, because it is the mixed product, which is always 0 or 1. Q.E.D.

Definition 3.4. Given a basis $\varepsilon = (e_1, e_2, e_3)$, if $u = u_1e_1 + u_2e_2 + u_3e_3$, with $u_1, u_2, u_3 \in \mathbb{F}_2$, then we define the *vector of coordinates* with respect to ε, and the *Squaring vector* (a vector in $\mathbb{F}_8^3$):

$$\mathrm{Coord}_\varepsilon(u) = [u]_\varepsilon = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}, \qquad [u]_{\mathrm{sq}} = \begin{bmatrix} u \\ u^2 \\ u^4 \end{bmatrix}.$$

Definition 3.5. Two bases $\varepsilon = (e_1, e_2, e_3)$ and $\varepsilon^* = (e_1^*, e_2^*, e_3^*)$ are *dual* if $\mathrm{tr}(e_i^* e_j) =< e_i^*, e_j >= \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker symbol (with value 1 if $i = j$, and 0 if $i \neq j$). This exactly means that $M_{\varepsilon^*}^{\mathrm{T}} M_\varepsilon = I_3$, i.e.

$$M_\varepsilon^{-1} = M_{\varepsilon^*}^{\mathrm{T}}.$$

A basis $\varepsilon = (e_1, e_2, e_3)$ is said to be *strictly auto-dual* if $\mathrm{tr}(e_i e_j) = \delta_{i,j}$, and *auto-dual* if, for a permutation σ on $\{1, 2, 3\}$, ε and $\varepsilon_\sigma = (e_{\sigma 1}, e_{\sigma 2}, e_{\sigma 3})$ are dual, i.e. such that $\mathrm{tr}(e_i e_j^*) = \delta_{i,j}$, with $e_j^* = e_{\sigma(j)}$.

Proposition 3.6. If $\varepsilon = (e_1, e_2, e_3)$ is a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$, the unique dual basis is given by $\varepsilon^* = (e_1^*, e_2^*, e_3^*)$ with:

$$e_1^* = e_2 \times e_3, \quad e_2^* = e_3 \times e_1, \quad e_3^* = e_1 \times e_2,$$

we have $(\varepsilon^*)^* = \varepsilon$ i.e.

$$e_1 = {e_2}^* \times {e_3}^*, \quad e_2 = {e_3}^* \times {e_1}^*, \quad e_3 = {e_1}^* \times {e_2}^*.$$

The coordinates of $u = u_1e_1 + u_2e_2 + u_3e_3$ are:

$$u_1 = \mathrm{tr}(ue_1^*),\ u_2 = \mathrm{tr}(ue_2^*),\ u_3 = \mathrm{tr}(ue_3^*).$$

In particular we have:

$$e_i^* = \sum_{j=1,2,3} < e_i^*, e_j^* > e_j, \quad e_i = \sum_{j=1,2,3} < e_i, e_j > e_j^*.$$

Proposition 3.7. 1 — Given a basis $\varepsilon = (e_1, e_2, e_3)$, we introduce

$$\mathrm{C}_\varepsilon = \mathrm{C}_{e_1e_2e_3} = \begin{bmatrix} e_2^4e_3^2 + e_2^2e_3^4 & e_2e_3^4 + e_2^4e_3 & e_2^2e_3 + e_2e_3^2 \\ e_3^4e_1^2 + e_3^2e_1^4 & e_3e_1^4 + e_3^4e_1 & e_3^2e_1 + e_3e_1^2 \\ e_1^4e_2^2 + e_1^2e_2^4 & e_1e_2^4 + e_1^4e_2 & e_1^2e_2 + e_1e_2^2 \end{bmatrix}.$$

For any $u = u_1e_1 + u_2e_2 + u_3e_3$, with $u_1, u_2, u_3 \in \{0, 1\}$,

$$\mathrm{Coord}_\varepsilon(u) = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \mathrm{C}_{e_1e_2e_3} \begin{bmatrix} u \\ u^2 \\ u^4 \end{bmatrix},$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

or briefly:

$$[u]_\varepsilon = C_\varepsilon [u]_{\mathrm{sq}}.$$

2 — In particular, for the canonical basis $\kappa = (R, S, I)$, if $u = xR + yS + zI$, with $x, y, z \in \{0, 1\}$,

$$\mathrm{Coord}_\kappa(u) = \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \mathrm{C}_{RSI} \begin{bmatrix} u \\ u^2 \\ u^4 \end{bmatrix}, = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix} \begin{bmatrix} u \\ u^2 \\ u^4 \end{bmatrix}.$$

with the notation from Proposition 2.7 for the circular involution C_{RSI}, or briefly:

$$[u]_\kappa = C_{RSI} [u]_{\mathrm{sq}}.$$

3 — With $M_\varepsilon = [\mathrm{Coord}_\kappa(e_1)|\mathrm{Coord}_\kappa(e_2)|\mathrm{Coord}_\kappa(e_3)]$ we have

$$\mathrm{Coord}_\kappa(u) = M_\varepsilon \mathrm{Coord}_\varepsilon(u),$$

or

$$[u]_\kappa = M_\varepsilon [u]_\varepsilon.$$

Hence

$$\mathrm{C}_{e_1e_2e_3} = {M_\varepsilon}^{-1} \mathrm{C}_{RSI} = {M_\varepsilon^*}^{\mathrm{T}} \mathrm{C}_{RSI}$$

Proof. From Proposition 3.2 and Definition 3.1 we get $u_1 =< u, e_2 \times e_3 >= \mathrm{tr}(u(e_2 \times e_3)) = \mathrm{tr}(u(e_2e_3(e_2 + e_3))^2)$, and we conclude with the value $\mathrm{tr}(w) = w + w^2 + w^4$ from Definition 2.3:

$$u_1 = u(e_2^4 e_3^2 + e_2^2 e_3^4) + u^2(e_2 e_3^4 + e_2^4 e_3) + u^4(e_2^2 e_3 + e_2 e_3^2).$$

In fact (see [5, Proposition 6.1]) $(-)_1$ is the indicator or characteristic function of the subset $\{e_1, e_1 + e_2, e_1 + e_3, e_1 + e_2 + e_3\}$, and it could be computed using this. For x, y, z in the case of the canonical basis, a direct checking is easy. With the exchange of coordinates given by $\mathrm{Coord}_\kappa(u) = M_\varepsilon \mathrm{Coord}_\varepsilon(u)$, and $\begin{bmatrix} u \\ u^2 \\ u^4 \end{bmatrix} = \mathrm{C}_{RSI} \mathrm{Coord}_\kappa(u)$ we obtain ${M_\varepsilon}^{-1} = \mathrm{C}_{e_1e_2e_3} \mathrm{C}_{RSI}$.

Q.E.D.

3.2 Characteristic linear relations between a basis in $\mathbb{F}_8$ and its dual

A basis and its dual are related by bilinear conditions; but these conditions could be expressed as follows by a system of linear conditions (a linear system).

Proposition 3.8. Given a basis $\varepsilon = (e_1, e_2, e_3)$ ans its dual $\varepsilon^* = (e_1^*, e_2^*, e_3^*)$ we have

$$e_1^* e_1 + e_2^* e_2 + e_3^* e_3 = 1,$$

$$e_1^{*2} e_1 + e_2^{*2} e_2 + e_3^{*2} e_3 = 0,$$

$$e_1^{*4} e_1 + e_2^{*4} e_2 + e_3^{*4} e_3 = 0.$$

These conditions determine ε for a given ε^*.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proof. The first proposed sum is $(e_2\times e_3)e_1+\cdots = e_2^2e_3^2(e_2^2+e_3^2)e_1+\cdots = e_1e_2e_3(e_2^3e_3+e_2e_3^3)+\cdots = e_1e_3e_3(e_2+e_3)(e_3+e_1)(e_1+e_3)(e_1+e_2+e_3) = 1$ (see Propositions 3.2 and 3.3). The third sum is $(e_2\times e_3)^4e_1+\cdots = e_2e_3(e_2+e_3)e_1+\cdots = e_1e_2e_3(e_2+e_3)+\cdots = 0$. If in the third formula we exchange the e_i and the e_i^*, and if we put it at the power 2, then we get the second formula. Finally we remark that the Cramer's formulas furnish $e_1 = e_2^{*2}e_3^{*2}(e_2^{*2}+e_2^{*2})$, hence $e_1 = e_2^*\times e_3^*$, etc. Q.E.D.

Proposition 3.9. Given a basis $\varepsilon = (e_1, e_2, e_3)$ and its dual $\varepsilon^* = (e_1^*, e_2^*, e_3^*)$, then $\varepsilon^{(2)} = (e_1^2, e_2^2, e_3^2)$ and $\varepsilon^{(4)} = (e_1^4, e_2^4, e_3^4)$ are bases, with dual the bases $\varepsilon^{*(2)} = (e_1^{*2}, e_2^{*2}, e_3^{*2})$ and $\varepsilon^{*(4)} = (e_1^{*4}, e_2^{*4}, e_3^{*4})$.

Proof. If $\varepsilon = (e_1, e_2, e_3)$ is a basis, so is $\varepsilon^{(2)} = (e_1^2, e_2^2, e_3^2)$, because $(-)^2$ is linear invertible. In Proposition 3.8 we can take the power 2 of each equation, to obtain the characterization of $\varepsilon^{(2)}$ from $\varepsilon^{*(2)}$. Q.E.D.

3.3 Parametrization (t, p) for unordered bases in $\mathbb{F}_8$

Proposition 3.10. A data $\varepsilon = (e_1, e_2, e_3)$ is a basis if and only if e_1, e_2, e_3 are the 3 roots in $\mathbb{F}_8$ of an equation with coefficients in $\mathbb{F}_8$

$$X^3 + tX^2 + qX + p = 0,$$

with

$$p, t \neq 0, \quad q = \frac{p^2t+1}{pt^2}.$$

The 2 parameters t and p *are not independent* if they correspond to an equation coming from a basis. Their precise relation is given in Proposition 3.15.

Proof. If $P_\varepsilon(X) := (X-e_1)(X-e_2)(X-e_3) \equiv X^3+tX^2+qX+p$ with

$$t = e_1+e_2+e_3, \quad p = e_1e_2e_3, \quad q = e_1e_2+e_2e_3+e_3e_1,$$

the condition in Proposition 3.3 means

$$ptP_\varepsilon(t) = 1,$$

i.e. $pt(qt+p) = 1$, i.e. $q = \frac{p^2t+1}{pt^2}$. Conversely, if $X^3+tX^2+qX+p = 0$ as 3 roots in $\mathbb{F}_8$, e_1, e_2 and e_3, with the given conditions on t, p, q, then we recover $e_1e_2e_3(e_1+e_2)(e_2+e_3)(e_3+e_1)(e_1+e_2+e_3) = 1$, and so (e_1, e_2, e_3) is a basis, and in particular these roots are not equal. Q.E.D.

3.4 The 28 unordered bases and the 4 auto-dual bases in $\mathbb{F}_8$

An element u is said to be *normal* over $\mathbb{F}_2$ if (u, u^2, u^4) is a basis, which is called a *normal basis*. If furthermore u is *primitive*, i.e. if the powers of u generate $\mathbb{F}_8\backslash\{0\}$, then the basis is said to be *normal primitive*. See [7], [8].

Proposition 3.11. There are 28 unordered bases of $\mathbb{F}_8$, or 168 when the order of terms is specified. These bases correspond to elements of $\mathrm{GL}_3(\mathbb{F}_2)$, i.e. 3×3 invertible matrices with coefficients in $\mathbb{F}_2$.

1 — Up to a circular permutation, there is only one *normal basis*:

$$\kappa = (R, S, I) = \kappa^*,$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

which is even a *normal primitive basis*. Up to a circular permutation, this κ is also the only *strictly auto-dual basis*.
2 — There are 3 other auto-dual bases (not strict), which are:

$$r = (R', I', 1), \quad s = (1, S', R') \quad i = (S', 1, I'),$$

associated to the matrices r, s, i in Definition 2.5 and Proposition 2.6; each one being its own dual, but with another order of terms:

$$r^* = (I', R', 1), \quad s^* = (1, R', S'), \quad i^* = (I', 1, S').$$

3 — Up to the order of terms, each basis $\varphi = (f_1, f_2, f_3)$ is of the form

$$\varphi = m\beta := (me_1, me_2, me_3),$$

with $\beta = (e_1, e_2, e_3)$ one of the four auto-dual bases κ, r, s or i, and $m \neq 0$.
4 — For any basis $\varepsilon = (e_1, e_2, e_3)$ we introduce $t_\varepsilon := e_1 + e_2 + e_3$. We have $t_\kappa = 1, t_r = R, t_s = S, t_i = I$, and the 4 bases ε with $t_\varepsilon = 1$ are $t_\beta^{-1}\beta$, with $\beta \in \{\kappa, r, s, i\}$, i.e.

$$\kappa = (R, S, I), R'r = (S', S, R'), S's = (S', I', I), I'i = (R, I', R').$$

5 — If $\varepsilon = (e_1, e_2, e_3)$ is a basis, and if $\varphi = \lambda\varepsilon$, with $\lambda \neq 0$, then $\varphi^* = \lambda^{-1}\varepsilon^*$. If $\varphi = m\beta$ as in the point 3, then $t_{\varphi^*} = m^{-2}t_\varphi$, and φ is auto-dual if and only if $t_{\varphi^*} = t_\varphi$.

Proof. For the parts 1 to 3, see [3] and [5, Proposition 6.2]. The part 4 is easy to check. For 5, as $e_1^* = e_2 \times e_3$, we have $f_1^* = \lambda e_2 \times \lambda e_3 = (\lambda e_2 \lambda e_3)^2(\lambda^2 e_2^2 + \lambda^2 e_3^2) = \lambda^6((e_2 e_3)^2(e_2^2 + e_3^2)) = \lambda^6 e_1^* = \lambda^{-1}e_1^*$. Then from $\varphi = m\beta$ we deduce $\varphi^* = m^{-1}\beta^* = m^{-1}\beta$ (as unordered bases), hence $t_{\varphi^*} = m^{-1}t_\beta$. As from $\varphi = m\beta$ we deduce $t_\varphi = mt_\beta$, we conclude $t_{\varphi^*} = m^{-2}t_\varphi$.
Nota bene: The part 3 will be completed in Proposition 3.14, with respect to the parameters t and a introduced in Section 3.5. Q.E.D.

3.5 True and Association for a basis, the independent parameters (t, a)

In this sub-section we show how unordered bases could be parametrized by two independent parameters, t and a, and we use that to organize a table of values for the 28 unordered bases.

Proposition 3.12. Let $a \in \{0, R, S, I\}$ and $t \neq 0$, i.e. a and t such that

$$a^4 + a^3 + a = 0, \quad t^7 = 1.$$

We introduce

$$q = at^2, \quad p = (a^2 + 1)t^3;$$

Then for each of the 28 basis $\varepsilon = (e_1, e_2, e_3)$, the set $\{e_1, e_2, e_3\}$ is the set of solutions of exactly one of the 28 equations

$$X^3 + tX^2 + at^2X + (a^2 + 1)t^3 = 0,$$

with in fact

$$t = e_1 + e_2 + e_3, \ , q = e_1e_2 + e_2e_3 + e_3e_1, \ p = e_1e_2e_3, \ a = \frac{e_1e_2 + e_2e_3 + e_3e_1}{(e_1 + e_2 + e_3)^2}.$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

We notice that

$$q = t^2 + p^4 t^4.$$

The unique $a = \frac{q}{t^2}$ corresponding to a given basis ε is named the *association* parameter of ε, denoted by $a = a_\varepsilon$. The parameter $t = t_\varepsilon$ is the *true*. These parameters are independent.

Proof. At first we see that if $t \neq 0$, $\varepsilon = (e_1, e_2, e_3)$, $\lambda\varepsilon = (\lambda e_1, \lambda e_2, \lambda e_3)$, and if we adopt the notations $t = t_\varepsilon$, $q = q_\varepsilon$, $p = p_\varepsilon$ in Proposition 3.10, we have $P_{\lambda\varepsilon}(X) = X^3 + \lambda t_\varepsilon X^2 + \lambda^2 q_\varepsilon X, + \lambda^3 p_\varepsilon$, hence

$$t_{\lambda\varepsilon} = \lambda t_\varepsilon, \;\; q_{\lambda\varepsilon} = \lambda^2 q_\varepsilon, \;\; p_{\lambda\varepsilon} = \lambda^3 p_\varepsilon.$$

Then, by Proposition 3.11 we have the 4 bases with $t = 1$, the $t_\beta^{-1}\beta$, namely $\kappa = (R, S, I)$, $R'r = (S', S, R')$, $S's = (S', I', I)$, and $I'i = (R, I', R')$, of which the associated polynomials P_κ, $P_{R'r}$, $P_{S's}$, $P_{I'i}$ are:

$$X^3 + X^2 + 1, \;\; X^3 + X^2 + SX + R', \;\; X^3 + X^2 + IX + S', \;\; X^3 + X^2 + RX + I'.$$

We remark that

$$0^2 + 1 = 1, \;\; S^2 + 1 = R', I^2 + 1 = S', R^2 + 1 = I'.$$

So according to Proposition 3.11, each basis φ is multiple by a λ of one of the auto-dual bases, but also it is a multiple, by another λ (which in fact is t_φ), of one of the 4 bases for which $t = 1$ (which in fact is $t_\varphi^{-1}\varphi$) and then the corresponding polynomial is an element of one of the 4 families (with $\lambda \neq 0$):

$$X^3 + \lambda X^2 + \lambda^3, \;\; X^3 + \lambda X^2 + \lambda^2 SX + \lambda^3 R',$$
$$X^3 + \lambda X^2 + \lambda^2 IX + \lambda^3 S', \;\; X^3 + \lambda X^2 + \lambda^2 RX + \lambda^3 I'.$$

Finally we observe that in each family written as $X^3 + tX^2 + qX + p$ we have

$$\left(\frac{q}{t^2}, \frac{p}{t^3}\right) \in \{(0,1), (S, R'), (I, S'), (R, I')\},$$

and so

$$\left(\frac{q}{t^2}\right)^2 + 1 = \frac{p}{t^3},$$

or equivalently

$$q = t^2 + p^4 t^4.$$

So if we define a by $a = \frac{q}{t^2}$, we have $p = (a^2+1)t^3$. Then $pt(qt+p) = (a^2+1)t^4(at^3 + (a^2+1)t^3) = (a^2+1)(a^2+a+1)$. So we recover the property $q = \frac{p^2 t+1}{pt^2}$ of Proposition 3.10, i.e. $pt(qt+p) = 1$, exactly if $a^4 + a^3 + a = 0$. Thus this Proposition 3.12 refines Proposition 3.10.
These parameters are independent, because t takes 7 values, a takes 4 values, and $28 = 7 \times 4$ is the number of bases. Q.E.D.

Proposition 3.13. The 168 bases of $\mathbb{F}_8$ over $\mathbb{F}_2$ are permutations of 28 bases which are the 4 auto-dual bases κ, r, s, i, and their multiples, distributed as follows, according to Proposition 3.11,

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

with respect to the two independent parameters t and a from Proposition 3.12:

	$a=0$	$a=R$	$a=S$	$a=I$
$t=1$	$\kappa=\mathbf{R},\mathbf{S},\mathbf{I}$	$I'i=R,I',R'$	$R'r=S',S,R'$	$S's=S',I',I$
$t=R$	$R\kappa=S,I',S'$	$Ii=S,I,1$	$\mathbf{r}=\mathbf{R}',\mathbf{I}',\mathbf{1}$	$R's=R',I,S'$
$t=S$	$S\kappa=I',I,R'$	$S'i=I',S',R$	$Rr=1,I,R$	$\mathbf{s}=\mathbf{1},\mathbf{S}',\mathbf{R}'$
$t=I$	$I\kappa=S',R',R$	$\mathbf{i}=\mathbf{S}',\mathbf{1},\mathbf{I}'$	$I'r=S,R',I'$	$Ss=S,1,R$
$t=R'$	$R'\kappa=1,R,I'$	$Si=1,S,S'$	$S'r=I,R,S'$	$Is=I,S,I'$
$t=S'$	$S'\kappa=R',1,S$	$Ri=R',R,I$	$Ir=I',1,I$	$I's=I',R,S$
$t=I'$	$I'\kappa=I,S',1$	$R'i=I,R',S$	$Sr=R,S',S$	$Rs=R,R',1$

Proof. If $\varphi=\lambda\varepsilon$, we have $a_\varphi=\frac{q_\varphi}{t_\varphi{}^2}=\frac{\lambda^2 q_\varepsilon}{(\lambda t_\varepsilon)^2}=a_\varepsilon$. For the 4 bases with $t=1$ we have

$$a_\kappa=0,\quad a_{R'r}=S,\quad a_{S's}=I,\quad a_{I'i}=R.$$

We check this table with the multiplication table of $\mathbb{F}_8$ given in Definition 2.1. If we consider an ordered basis $\varepsilon=(e_1,e_2,e_3)$ as a vector $\vec{\varepsilon}=\begin{bmatrix}e_1\\e_2\\e_3\end{bmatrix}$ of $\mathbb{F}_8^3$, it is a part of the table of multiplication by scalars in $\mathbb{F}_8^3$. Q.E.D.

3.6 Resolution of $\varphi=m\beta$, parameters (m,Q), dependence for (t,p)

Using the parameters t and a we solve $\varphi=m\beta$ and we analyze the exact dependance between t and p introduced in Proposition 3.10.

Proposition 3.14. Given a basis φ, with parameters t and a, the unique auto-dual basis β and unique coefficient m such that $\varphi=m\beta$ are given by

$$t_\beta=a^2+a+1,\quad a_\beta=a,\quad m=t(a^2+1).$$

If we introduce the parameter $Q_\varphi=\frac{tq}{p}$ then $Q_\varphi=Q_\beta:=Q$, and (m,Q) is another parametrization for bases φ, with independent parameters, related to the parametrization with (t,a) by:

$$m=t(a+1)^2,Q=a^5,\quad t=m(Q+1)^4,a=Q^3.$$

The constraint for a,

$$a^4+a^3+a=0,$$

is now equivalent to the constraint for Q:

$$\mathrm{tr}(Q):=Q^4+Q^2+Q=0.$$

Proof. Let $\beta\in\{\kappa,r,s,i\}$ be an auto-dual basis, t_β the associated value of t, and $X^3+t_\beta X^2+q_\beta X+p_\beta=0$ the corresponding equation. If $\lambda\neq 0$ and $\varphi=\lambda\beta$, the associated equation is $X^3+t_\varphi X^2+q_\varphi X+p_\varphi=0$, with $t_\varphi=\lambda t_\beta$, $q_\varphi=\lambda^2 q_\beta$, $p_\varphi=\lambda^3 p_\beta$, and

$$Q_\varphi:=\frac{t_\varphi q_\varphi}{p_\varphi}=\frac{t_\beta q_\beta}{p_\beta}=Q_\beta:=Q;\quad a_\varphi=\frac{q_\varphi}{t_\varphi^2}=\frac{q_\beta}{t_\beta^2}=a_\beta:=a.$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

From $a^4 = a^3 + a$, we deduce $a^6 = a^2 + a$, $(a^2+1)^6 = a^6 + 1$, and then, as $a = \frac{q}{t^2}$, $q = at^2$, $p = (a^2+1)t^3$, we have $Q = \frac{tq}{p} = \frac{a}{a^2+1} = a(a^2+1)^6$, $Q = a^3 + a^2 + a$, $Q = a^5$. Furthermore $Q^4 + Q^2 + Q = 0$.
We verify that, for any auto-dual basis β, we have $Q_\beta = t_\beta^2 + 1$ and $t_\beta = Q_\beta^4 + 1 = Q^4 + 1$, $t_\beta = (a^3 + a^2 + a)^4 + 1 = a^2 + a + 1$. Then we obtain $t_\beta^{-1} = a^2 + 1$. If $\varphi = m\beta$ we have $t_\varphi = mt_\beta$, $m = t_\varphi t_\beta^{-1}$, $m = t(a^2+1)$.
$Q = a^5$ is equivalent to $a = Q^3$. To obtain $t = t_\varphi$, starting with $t_\varphi = mt_\beta = m(a^2 + a + 1)$, as $a^2 + a + 1 = Q^6 + Q^3 + 1 = Q^4 + 1 = (Q+1)^4$, we obtain $t = m(Q+1)^4$. Q.E.D.

Proposition 3.15. Given a basis $\varphi = (e_1, e_2, e_3)$ determined — as an unordered basis — as the solution of $X^3 + tX^2 + qX + p$ as in Proposition 3.10, then, with the notations of Proposition 3.14, we have

$$Q = \frac{tq}{p} = \frac{1}{p^2 t} + 1.$$

Not only q is determined by t and p, but t and p themselves are *not independent*, they have exactly to satisfy to

$$p^2 t \in \{1, R', S', I'\}, \quad \text{or equivalently} \quad pt^4 + p^6 t^3 + p^4 t^2 = 1.$$

Other equivalent equations are

$$p^5 t^6 + pt^4 + p^2 t = 1, \quad \text{as well as} \quad p^3 t^5 + p^4 t^2 + p^2 t = 1.$$

And we have the equivalent condition

$$< p^3 t^5, p^3 t^5 >= 1, \quad \text{or equivalently} \quad p^3 t^5 \in \{1, R, S, I\}.$$

Proof. If $Q = \frac{tq}{p}$, from $q = \frac{1+p^2 t}{pt^2}$ we obtain $Q = \frac{1}{p^2 t} + 1$.
Of course each of these equations implies that $t, p \neq 0$. The first equation is the same as $(p^2 t)^4 + (p^2 t)^3 + (p^2 t)^2 = 1$, which expresses that $p^2 t$ is a solution of $X^4 + X^3 + X^2 = 1$, i.e. of $(X+1)(X^3 + X + 1) = 0$, i.e. an element of $\{1, R', S', I'\}$, and this means that $\frac{1}{p^2 t} \in \{1, R, S, I\}$, that is to say $\frac{1}{p^2 t} + 1 = Q \in \{0, R', S', I'\}$; but this is proved by $\mathrm{tr}(Q) = 0$.
To obtain the second proposed equation we equalize the two expressions for q from Proposition 3.10 and Proposition 3.12: $q = \frac{1+p^2 t}{pt^2}$ and $q = t^2 + p^4 t^4$. To obtain the third equation we equalize the two expressions for pt^4 which appear in the two first equations. And for the final equation, we add the three first equations, this gives $p^3 t^5 + p^5 t^6 + p^6 t^3 = 1$, i.e. $\mathrm{tr}(p^3 t^5) = 1$, i.e. $< p^3 t^5, p^3 t^5 >= 1$. This last point can be deduced from $(p^2 t)^{-1} = (p^3 t^5)^4$. Q.E.D.

3.7 Parameters (t, k), dual parameters (t, c), geometrical duality in logics

Proposition 3.16. With the notations of Proposition 3.14 and $m = k^{-1}$, a basis φ — except for the order of its terms — is associated to a unique pair $(t, k) \in \left(\mathbb{F}_8 \backslash \{0\}\right)^2$ of parameters such that

$$< t, k >= 1.$$

There are $7 \times 4 = 28$ such (t, k). Furthermore if φ is represented by (t, k) then its dual φ^* is represented by $(t, k)^* := (c, l)$, with $c = k^2 t, l = k^{-1}$:

$$(t, k)^* = (k^2 t, k^{-1}).$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proof. From $t = m(Q+1)^4$ in Proposition 3.14, we deduce $\left(\frac{t}{m}\right)^2 + 1 = Q$, and $< t, k >= \mathrm{tr}\left(\frac{t}{m}\right) = \mathrm{tr}(Q)+1 = 0+1 = 1$. Given (t,k) we recover β by $t_\beta = tk$, and a or Q by $a = \frac{1}{(tk)^4}+1$, $Q = (tk)^2+1$. For the duality, if $\varphi = m\beta$ as in Proposition 3.14, we know by Proposition 3.11 that $\varphi^* = m^{-1}\beta^* = m^{-1}\beta$ (up to an order among the vectors in the basis), and $m_{\varphi^*} = {m_\varphi}^{-1} = m^{-1}$, i.e. $l = k^{-1}$, and $t_{\varphi^*} = {m_\varphi}^{-2} t_\varphi = m^{-2}t = k^2 t$, i.e. $c = k^2 t$. Q.E.D.

Definition 3.17. Given a basis φ with dual φ^*, then the true t_{φ^*} is also named the *co-true* of φ and denoted by $c_\varphi = t_{\varphi^*}$. The couple (t_φ, c_φ) is named the couple of *dual parameters*.

Proposition 3.18. 1 — If φ — as an unordered basis — is parametrized by t, q, p, it could be parametrized by (t_φ, c_φ), with $t_\varphi = e_1 + e_2 + e_3$ and $c_\varphi = t_{\varphi^*} = e_1^* + e_2^* + e_3^*$, as in Definition 3.17, with in fact

$$c_\varphi = p^5 t^5,$$

and then $< t_\varphi, c_\varphi >= 1$.

2 — Conversely, given $(t,c) \in \left(\mathbb{F}_8 \backslash \{0\}\right)^2$, a couple of of parameters such that

$$< t, c >= 1,$$

there is exactly one unordered basis φ, denoted by $\varphi = (t,c)$, with $t_\varphi = t$, $c_\varphi = c$, which is determined by

$$t = t, \quad a = c^5 t^5 + 1.$$

Then φ^* is represented by (c,t), i.e.

$$(t,c)^* = (c,t).$$

The other parameters, for φ and φ^*, are

$$m = c^3 t^4, \;\; Q = c^2 t^2 + c^4 t^4, \;\; q = c^5 + t^2, \;\; p = c^3 t^6.$$

$$t^* = c, \quad c^* = t, \quad a^* = c^5 t^5 + 1 = a,$$

$$m^* = c^4 t^3, \;\; Q^* = c^2 t^2 + c^4 t^4, \;\; q^* = c^2 + t^5, \;\; p^* = c^6 t^3.$$

3 — Starting from (t,q,p) for φ, we obtain (t^*, q^*, p^*) for φ^*, with

$$t^* = p^5 t^5, \quad q^* = p^3 t^3 + t^5, \quad p^* = p^2 t^5.$$

Proof. With the notations of Proposition 3.16 let φ be a basis, its various parameters being t, c, q, p, a, Q, m, k, and let φ^* its dual, with parameters denoted by $t^*(= c)$, $c^*(= t)$, q^*, p^*, a^*, Q^*, m^*, k^*. We have $c_{\varphi^*} = t_\varphi$, as $(\varphi^*)^* = \varphi$.

Starting with the data φ and the associated t, q, p, we compute c. We have $\varphi^* = (e_2 \times e_3, e_3 \times_1, e_1 \times e_2)$, $t_{\varphi^*} = e_2 \times e_3 + e_3 \times e_1 + e_1 \times e_2 = e_2^2 e_3^2 (e_2 + e_3)^2 + \cdots = (e_2 e_3 (e_2 + e_3) + \dots)^2$, hence the value of $c_\varphi = t_{\varphi^*}$ is given by ${c_\varphi}^4 = {t_{\varphi^*}}^4 = e_2 e_3 (e_2 + e_3) + \cdots = e_2^2 e_3 + e_2 e_3^2 \dots$. Computing $t_\varphi q_\varphi + p_\varphi = (e_1 + \dots)(e_2 e_3 + \dots) + e_1 e_2 e_3$ we obtain exactly this $e_2^2 e_3 + e_2 e_3^2 \dots$, and so: ${c_\varphi}^4 = t_\varphi q_\varphi + p_\varphi$. But we know that $tq + p = (pt)^{-1} = (pt)^6$, ${c_\varphi}^4 = (p_\varphi t_\varphi)^6$, and $c_\varphi = (p_\varphi t_\varphi)^5$, or briefly $c = (tq+p)^2 = (pt)^5$. Hence we have $tc = t^6 p^5 = (t^5 p^3)^4$, and in Proposition 3.15 we proved that the trace of that expression is 1, i.e. $< t, c >= 1$.

All the parameters of φ and φ^* could be expressed with $t = t_\varphi$ and $c = c_\varphi = t^*$, as follows. From

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 3.16 we know that $k^* = k^{-1}$, $c = t^* = k^2 t$. From $c = k^2 t$ we obtain $m^2 = k^{-2} = tc^{-1}$, $m = c^3 t^4$; but also by Proposition 3.14 we have $m = t(a^2+1)$, $m^2 = t^2(a^4+1)$, and $a^4+1 = (tc)^{-1}$, $a = (tc)^{-2} + 1 = (tc)^5 + 1$.
We have $a^2 + 1 = (tc)^{-4}$, $Q = \frac{a}{a^2+1} = (tc)^2 + (tc)^4$. From $q = at^2$ we obtain $q = c^{-2} + t^2 = c^5 + t^2$, and from $p = (a^2+1)t^3$ we obtain $p = (tc)^{-4}t^3 = t^{-1}c^{-4} = c^3 t^6$.
We have $t^* = c = p^5 t^5$. By duality, exchanging φ and φ^*, we have also, with $p_{\varphi^*} = p^*$, $t = (p^* c)^5$, $p*^5 = tc^2$, $p^* = (tc^2)^3 = t^3 c^6 = t^3 (p^5 t^5)^6$, $p^* = p^2 t^5$. And finally we have $q^* = c^2 + t^5 = (p^5 t^5)^2 + t^5 = p^3 t^3 + t^5$. Q.E.D.

Proposition 3.19. For any of the 28 bases of $\mathbb{F}_8$ as given in the table of Proposition 3.13, the only relation between its *true* t and its *co-true* c, and its *association* parameter a, is given by

$$a = (ct)^5 + 1 \in \{0, R, S, I\}, \quad \text{or} \quad ct = (a+1)^3 = a^4 + a^2 + 1 \in \{1, R, S, I\},$$

and the table of values of $c = c(t, a) = \frac{(a+1)^3}{t}$ is

$c(t,a)$	$a = 0$	$a = R$	$a = S$	$a = I$
$t = 1$	$\mathbf{c_\kappa = 1}$	$c_{I'i} = R$	$c_{R'r} = S$	$c_{S's} = I$
$t = R$	$c_{R\kappa} = R'$	$c_{Ii} = 1$	$\mathbf{c_r = R}$	$c_{R's} = I'$
$t = S$	$c_{S\kappa} = S'$	$c_{S'i} = R'$	$c_{Rr} = 1$	$\mathbf{c_s = S}$
$t = I$	$c_{I\kappa} = I'$	$\mathbf{c_i = I}$	$c_{I'r} = S'$	$c_{Ss} = 1$
$t = R'$	$c_{R'\kappa} = R$	$c_{Si} = S$	$c_{S'r} = I'$	$c_{Is} = S'$
$t = S'$	$c_{S'\kappa} = S$	$c_{Ri} = I'$	$c_{Ir} = I$	$c_{I's} = R'$
$t = I'$	$c_{I'\kappa} = I$	$c_{R'i} = S'$	$c_{Sr} = R'$	$c_{Rs} = R$

Proof. Clearly the 2 conditions are equivalent. We know that $ct = p^5 t^6$ (in the proof of Proposition 3.18), and $p = (a^2+1)t^3$ (Proposition 3.12), and so $ct = ((a^2+1)t^3)^5 t^6 = (a^2+1)^5 = (a^2+1)^{-2} = (a+1)^{-4} = (a+1)^3$; and this is $a^4 + a^2 + 1$ because $a^4 + a^3 + a = 0$. Then the condition $ct \in \{1, R, S, I\}$ comes from $a \in \{0, R, S, I\}$, and is equivalent to $< c, t >= 1$ or $\mathrm{tr}(ct) = 1$, given in Proposition 3.18. As a corollary we obtain the next Proposition 3.20. Q.E.D.

Proposition 3.20. The table of the 28 bases with given values for (t, c) is

	$c = 1$	$c = R$	$c = S$	$c = I$	$c = R'$	$c = S'$	$c = I'$
$t = 1$	κ	$I'i$	$R'r$	$S's$			
$t = R$	Ii	$\mathbf{r}$			$R\kappa$		$R's$
$t = S$	Rr		$\mathbf{s}$	$S'i$	$S\kappa$		
$t = I$	Ss'			$\mathbf{i}$		$I'r$	$I\kappa$
$t = R'$		$R'\kappa$	Si			$C^* : Is$	$B : S'r$
$t = S'$			$S'\kappa$	Ir	$C : I's$		$A^* : Ri$
$t = I'$		Rs		$I'\kappa$	$B^* : Sr$	$A : R'i$	

In this table we emphasize positions of the bases A, B, C and the dual bases $A^* = A^{\mathrm{T}}, B^* = B^{\mathrm{T}}, C^* = C^{\mathrm{T}}$. By $A : R'i$ we mean that as an unordered basis A is $R'i$, etc.

4 Logics on $\mathbb{F}_8$ and parametrizations of conjunctions

A basis is described by three parameters e_1, e_2, e_3, which have to be linearly independent and which are considered as unordered. But, for calculus with matrices, a basis is *given* as an ordered data $\varepsilon = (e_1, e_2, e_3)$. In the previous section we introduced parameters which in fact are associated to unordered bases, the two independent t and a, and the two t and c with the only dependence

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

$< t, c >= 1$. Starting from (t, c) we recover $a = (ct)^5 + 1$ and $ct = a^4 + a^2 + 1$.
This presentation has to be completed. In order to give explicit algebraic formulas for an arbitrary conjunction associated to an arbitrary basis, we need parameters directly related to the polynomial functions associated to conjunctions, the $\varepsilon_6, \varepsilon_5, \varepsilon_3$ introduced in Proposition 4.4; then we need to express these parameters with respect to (t, a) or to (t, c).
Slightly modified the $\varepsilon_6, \varepsilon_5, \varepsilon_3$ generate the canonical parameters ρ, σ, ι and the differential parameters d_6, d_5, d_3, emphasizing differences $\wedge_\varepsilon - \wedge$.

4.1 Logic associated to an arbitrary basis, associated polynomial coordinates

Definition 4.1. To each basis $\varepsilon = (e_1, e_2, e_3)$ of $\mathbb{F}_8$ is associated a Boolean structure $(\wedge_\varepsilon, \neg_\varepsilon)$ on $\mathbb{F}_8$ given as follows:
If $u = u_1e_1 + u_2e_2 + u_3e_3$ and $v = v_1e_1 + v_2e_2 + v_3e_3$, then

$$u \wedge_\varepsilon v = u_1v_1e_1 + u_2v_2e_2 + u_3v_3e_3, \quad \neg_\varepsilon u = (u_1 + 1)e_1 + (u_2 + 1)e_2 + (u_3 + 1)e_3.$$

With $\Delta_\varepsilon = \begin{bmatrix} e_1 & 0 & 0 \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{bmatrix}$ and $t_\varepsilon = e_1 + e_2 + e_3 = \mathrm{tr}(\Delta_\varepsilon)$, we have

$$u \wedge_\varepsilon v = \mathrm{Coord}_\varepsilon(u)^{\mathrm{T}} \Delta_\varepsilon \mathrm{Coord}_\varepsilon(v), \quad \neg_\varepsilon u = u + t_\varepsilon.$$

Nota bene : The logic associated to the basis ε is in fact associated only to the unordered basis $\{e_1, e_2, e_3\}$, hence we can hope to express it with t, a or with t, c.

Proposition 4.2. The logic associated to a basis $\varepsilon = (e_1, e_2, e_3)$ determines this basis, except for the order of its terms, because e_1, e_2 and e_3 are the atoms; for this logic the truth values are the 'false' $f = 0$, the 'true' $t_\varepsilon = e_1 + e_2 + e_3$, briefly denoted by t, and $\neg_\varepsilon u = u + t$, and, with $u \vee_\varepsilon v = \neg_\varepsilon(\neg_\varepsilon u \wedge_\varepsilon \neg_\varepsilon v)$, the sum $u + v$ is the 'symmetrical difference'

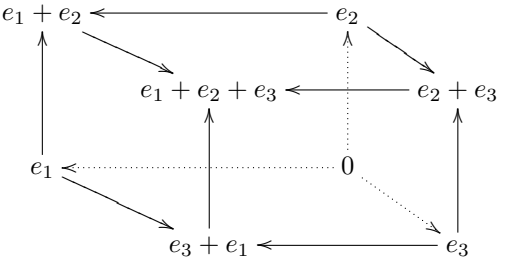
$$u + v = (\neg_\varepsilon u \wedge_\varepsilon v) \vee_\varepsilon (u \wedge_\varepsilon \neg_\varepsilon v).$$

Hence we obtain effectively 28 such logics.

Proposition 4.3. The logic associated to a basis $\varepsilon = (e_1, e_2, e_3)$ as in Definition 4.1 and Proposition 4.2 is determined by its associated order

$$u \leq_\varepsilon v \Leftrightarrow u \wedge_\varepsilon v = u,$$

and this order is a cube



Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 4.4. Given a basis $\varepsilon = (e_1, e_2, e_3)$ and its dual $\varepsilon^* = (e_1^*, e_2^*, e_3^*)$, the associated conjunction $\wedge_\varepsilon$ is given by

$$u \wedge_\varepsilon v = \varepsilon_8 u^4 v^4 + \varepsilon_6(u^2 v^4 + u^4 v^2) + \varepsilon_5(uv^4 + u^4 v) + \varepsilon_4 u^2 v^2 + \varepsilon_3(uv^2 + u^2 v) + \varepsilon_2 uv,$$

with, for $k \in \{2, 3, 4, 5, 6, 8\}$:

$$\varepsilon_k = \sum_{1 \le i \le 3} (e_i^*)^k e_i.$$

Also we have

$$u \wedge_\varepsilon v = \varepsilon_8 u^4 v^4 + \varepsilon_4 u^2 v^2 + \varepsilon_2 uv + \varepsilon_6(u \times v) + \varepsilon_5(u \times v)^2 + \varepsilon_3(u \times v)^4.$$

These coefficients — named *polynomial coordinates* of ε — will be precised in Proposition 4.5.

Proof. As u_1 is $\mathrm{tr}(ue_1^*) = ue_1^* + (ue_1^*)^2 + (ue_1^*)4$, the component $(u \wedge_\varepsilon v)_1$ of $u \wedge_\varepsilon v$ on e_1 is $(ue_1^* + (ue_1^*)^2 + (ue_1^*)^4)(ve_1^* + (ve_1^*)^2 + (ve_1^*)^4)$. By expansion, product with e_1, and summation with its analogous for the second and the third components, we obtain $\varepsilon_k = \sum_{1 \le i \le 3} (e_i^*)^k e_i$. The second formula is immediate from the formula $u \times v = u^2 v^2 (u^2 + v^2)$ from Proposition 3.2. Q.E.D.

Proposition 4.5. The conjunction $u \wedge_\varepsilon v$ is bilinear and symmetrical, and then it is characterized by the following conditions:

$$e_1 \wedge_\varepsilon e_1 = e_1, \quad e_2 \wedge_\varepsilon e_2 = e_2, \quad e_3 \wedge_\varepsilon e_3 = e_3,$$

$$e_1 \wedge_\varepsilon e_2 = e_2 \wedge_\varepsilon e_3 = e_3 \wedge_\varepsilon e_1 = 0.$$

So the coefficients ε_k are given by

$$\varepsilon_8 = 1, \varepsilon_4 = 0, \varepsilon_2 = 0$$

and the unique solution $(e_6, \varepsilon_5, \varepsilon_3)$ of the system

$$\varepsilon_6 e_1^* + \varepsilon_5 (e_1^*)^2 + \varepsilon_3 (e_1^*)^4 = (e_2 e_3)^4,$$

$$\varepsilon_6 e_2^* + \varepsilon_5 (e_2^*)^2 + \varepsilon_3 (e_2^*)^4 = (e_3 e_1)^4,$$

$$\varepsilon_6 e_3^* + \varepsilon_5 (e_3^*)^2 + \varepsilon_3 (e_3^*)^4 = (e_1 e_2)^4,$$

that is to say

$$\varepsilon_6 = (e_2 e_3)^4 e_1 + (e_3 e_1)^4 e_2 + (e_1 e_2)^4 e_3,$$

$$\varepsilon_5 = (e_2 e_3)^4 e_1^2 + (e_3 e_1)^4 e_2^2 + (e_1 e_2)^4 e_3^2,$$

$$\varepsilon_3 = (e_2 e_3)^4 e_1^4 + (e_3 e_1)^4 e_2^4 + (e_1 e_2)^4 e_3^4.$$

With these values we have:

$$u \wedge_\varepsilon v = u^4 v^4 + \varepsilon_6(u \times v) + \varepsilon_5(u \times v)^2 + \varepsilon_3(u \times v)^4.$$

The relations between these coefficients will be given in Proposition 4.13.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proof. In fact immediately we have $\varepsilon_8 = 1$, $\varepsilon_4 = 0$, $\varepsilon_2 = 0$, because of Proposition 3.8. Then the second formula in Proposition 4.4 becomes $u \wedge_\varepsilon v = u^4 v^4 + \varepsilon_6(u \times v) + \varepsilon_5(u \times v)^2 + \varepsilon_3(u \times v)^4$, and the 3 first conditions are satisfied; with $e_2 \times e_3 = e_1^*$, etc., the 3 next conditions mean exactly the proposed system. This system has a unique solution, because its determinant is 1, according to Proposition 3.2 in the case $u = e_1, u' = e_2, u'' = e_3$: in this case we have a basis, and so the value is 1 (see again [5, Propositions 4.1 et 4.3-4]). We compute the solution by Cramer formulas: ε_6, ε_5 and ε_3 are:
$(e_2e_3)^4({e_2^*}^2{e_3^*}^4 + {e_3^*}^2{e_2^*}^4) + (e_3e_1)^4({e_3^*}^2{e_1^*}^4 + {e_1^*}^2{e_3^*}^4) + (e_1e_2)^4({e_1^*}^2{e_2^*}^4 + {e_2^*}^2{e_1^*}^4)$,
$(e_2e_3)^4(e_2^*e_3^{*4} + e_3^*e_2^{*4}) + (e_3e_1)^4(e_3^*e_1^{*4} + e_1^*e_3^{*4}) + (e_1e_2)^4(e_1^*e_2^{*4} + e_2^*e_1^{*4})$, and $(e_2e_3)^4(e_2^*e_3^{*2} + e_3^*e_2^{*2}) + (e_3e_1)^4(e_3^*e_1^{*2} + e_1^*e_3^{*2}) + (e_1e_2)^4(e_1^*e_2^{*2} + e_2^*e_1^{*2})$. We conclude with $({e_2}^*{e_3}^*)^2({e_2}^* + {e_3}^*)^2 = {e_2}^* \times {e_3}^* = e_1$ etc. Q.E.D.

Proposition 4.6. 1 — With the notations of Proposition 4.5 we have

$$u \wedge_\varepsilon v = \begin{bmatrix} u & u^2 & u^4 \end{bmatrix} \begin{bmatrix} 0 & \varepsilon_3 & \varepsilon_5 \\ \varepsilon_3 & 0 & \varepsilon_6 \\ \varepsilon_5 & \varepsilon_6 & 1 \end{bmatrix} \begin{bmatrix} v \\ v^2 \\ v^4 \end{bmatrix},$$

and so the matrix $L_\varepsilon := \begin{bmatrix} 0 & \varepsilon_3 & \varepsilon_5 \\ \varepsilon_3 & 0 & \varepsilon_6 \\ \varepsilon_5 & \varepsilon_6 & 1 \end{bmatrix}$ is a representation of the $\mathbb{F}_2$-bilinear map

$$\wedge_\varepsilon : \mathbb{F}_8 \times \mathbb{F}_8 \to \mathbb{F}_8 : (u, v) \mapsto u \wedge_\varepsilon v.$$

We notice that $L_\kappa = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

Proof. Using Propositions 4.4 and 4.5 we expand the conjunction $u \wedge_\varepsilon v$ as $u^4(v^4 + \varepsilon_6 v^2 + \varepsilon_5 v) + u^2(\varepsilon_6 v^4 + \varepsilon_3 v) + u(\varepsilon_5 v^4 + \varepsilon_3 v^2)$. For L_κ, Proposition 2.8 gives $\kappa_6 = \kappa_3 = 1, \kappa_5 = 0$. Q.E.D.

Proposition 4.7. Given a basis ε we consider Δ_ε, K_ε, L_ε defined by

$$u \wedge_\varepsilon v = [u]_\varepsilon^{\mathrm{T}} \Delta_\varepsilon [v]_\varepsilon = [u]_\kappa^{\mathrm{T}} K_\varepsilon [v]_\kappa = [u]_{\mathrm{sq}}^{\mathrm{T}} L_\varepsilon [v]_{\mathrm{sq}},$$

with Δ_ε as in Definition 4.1 and L_ε as in Proposition 4.6, with notations of Definition 3.4 and Proposition 3.7. The third coefficient K_ε is named the *canonical matrix* of $\wedge_\varepsilon$, and we have:

$$L_\varepsilon = \mathrm{C}_{RSI} K_\varepsilon \mathrm{C}_{RSI}, \quad K_\varepsilon = {M_\varepsilon^{-1}}^{\mathrm{T}} \Delta_\varepsilon M_\varepsilon^{-1}, \quad L_\varepsilon = \mathrm{C}_\varepsilon^{\mathrm{T}} \Delta_\varepsilon \mathrm{C}_\varepsilon.$$

We notice that $K_\kappa = \begin{bmatrix} R & 0 & 0 \\ 0 & S & 0 \\ 0 & 0 & I \end{bmatrix}$.
K_ε will be considered again in Proposition 4.15.

Proof. We have seen that $[u]_\kappa = \mathrm{C}_{RSI}[u]_{\mathrm{sq}}$, $[u]_\varepsilon = \mathrm{C}_\varepsilon[u]_{\mathrm{sq}}$, $[u]_\kappa = M_\varepsilon[u]_\varepsilon$. From Proposition 4.6 we have $u \wedge_\varepsilon v = [u]_{\mathrm{sq}}^{\mathrm{T}} L_\varepsilon [v]_{\mathrm{sq}} = [u]_\kappa^{\mathrm{T}} \mathrm{C}_{RSI} L_\varepsilon \mathrm{C}_{RSI} [v]_\kappa$, and $\mathrm{C}_{RSI} L_\varepsilon \mathrm{C}_{RSI} = K_\varepsilon$. From Definition 4.1 we have $u \wedge_\varepsilon v = {[u]_\varepsilon}^{\mathrm{T}} \Delta_\varepsilon [v]_\varepsilon = {[u]_\kappa}^{\mathrm{T}} {M_\varepsilon^{-1}}^{\mathrm{T}} \Delta_\varepsilon M_\varepsilon^{-1} [v]_\kappa$, and ${M_\varepsilon^{-1}}^{\mathrm{T}} \Delta_\varepsilon M_\varepsilon^{-1} = K_\varepsilon$. Using Proposition 3.7 we have $\mathrm{C}_\varepsilon = M_\varepsilon^{-1} \mathrm{C}_{RSI}$, and $L_\varepsilon = \mathrm{C}_{RSI} {M_\varepsilon^{-1}}^{\mathrm{T}} \Delta_\varepsilon M_\varepsilon^{-1} \mathrm{C}_{RSI} = \mathrm{C}_\varepsilon^{\mathrm{T}} \Delta_\varepsilon \mathrm{C}_\varepsilon$. Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 4.8. If $\varepsilon = (e_1, e_2, e_3)$ is a basis, and $\lambda \neq 0$, then the conjunctions associated to ε and to $\lambda\varepsilon$ are related by $(\lambda\varepsilon)_i = \lambda^{1-i}\varepsilon_i$, for $i = 6, 5, 3$, i.e.:

$$u \wedge_\varepsilon v = u^4v^4 + \varepsilon_6(u \times v) + \varepsilon_5(u \times v)^2 + \varepsilon_3(u \times v)^4,$$

$$u \wedge_{\lambda\varepsilon} v = u^4v^4 + \lambda^2\varepsilon_6(u \times v) + \lambda^3\varepsilon_5(u \times v)^2 + \lambda^5\varepsilon_3(u \times v)^4.$$

Proof. With Proposition 3.11, if $\varphi = \lambda\varepsilon = (\lambda e_1, \lambda e_2, \lambda e_3) = (f_1, f_2, f_3)$, then $\varphi^* = \lambda^{-1}\varepsilon^*$, $f_1^* = \lambda^{-1}e_1^*$, $f_1^{*6} = \lambda^{-6}e_1^{*6}$, $\varphi_6 = f_1^{*6}f_1 + \cdots = \lambda^{-6}\lambda e_1^{*6}e_1 + \cdots = \lambda^{-5}\varepsilon_6 = \lambda^2\varepsilon_6$. Also $\varphi_5 = \lambda^{-4}\lambda\varepsilon_4 = \lambda^3\varepsilon_5$, $\varphi_3 = \lambda^{-2}\lambda\varepsilon_4 = \lambda^5\varepsilon_5$. Q.E.D.

Proposition 4.9. The coefficients of the conjunction $u \wedge_\varepsilon v$ associated to a basis $\varepsilon = (e_1, e_2, e_3)$, are given by

$$\varepsilon_6 = p^4t^4, \ \ \varepsilon_5 = p^2q^2, \ \ \varepsilon_3 = p^4.$$

Proof. From the values given in Proposition 4.5, with $\varepsilon_6 = (e_2e_3)^4e_1 + \ldots$ we obtain $\varepsilon_6^2 = e_2e_3e_1^2 + \cdots = e_1e_2e_3(e_1 + e_2 + e_3) = pt$. We have $\varepsilon_5 = (e_2e_3)^4e_1^2 + (e_3e_1)^4e_2^2 + (e_1e_2)^4e_3^2 = (e_1e_2e_3)^2(e_2^2e_3^2 + e_3^2e_1^2 + e_1^2e_2^2) = p^2q^2$. Of course $e_3 = (e_1e_2e_3)^4 = p^4$. Q.E.D.

Proposition 4.10. The conjunction $u \wedge_\varepsilon v$ associated to a basis $\varepsilon = (e_1, e_2, e_3)$ is given by

$$u \wedge_\varepsilon v = u^4v^4 + (a+1)t^2(u^2v^4 + u^4v^2) + at^3(uv^4 + u^4v) + (a+1)t^5(uv^2 + u^2v),$$

$$u \wedge_\varepsilon v = u^4v^4 + (a+1)t^2(u \times v) + at^3(u \times v)^2 + (a+1)t^5(u \times v)^4.$$

Proof. Using Proposition 4.9 and the values of p and q from 3.12, which are $q = at^2, p = (a^2+1)t^3$, we obtain, thanks to $a^4 = a^3 + a$ and consequently $a^6 = a^2 + a$:
$\varepsilon_6 = p^4t^4 = ((a^2+1)t^3)^4t^4 = (a+1)t^2$;
$\varepsilon_5 = p^2q^2 = (a^2+1)^2t^6a^2t^4 = (a^4+1)a^2t^3 = at^3$;
$\varepsilon_3 = p^4 = (a^2+1)^4t^{12} = (a+1)t^5$. Q.E.D.

Proposition 4.11. Given a basis ε, parametrized by its t, q, p or its t and a, or its 'true' t and its 'co-true' c, we have

$$\varepsilon_6 = p^4t^4 = (a+1)t^2 = c^5,$$
$$\varepsilon_5 = p^2q^2 = at^3 = c^5t + t^3,$$
$$\varepsilon_3 = p^4 = (a+1)t^5 = c^5t^3.$$

So the conjunctions associated to ε and to ε^* are given by:

$$u \wedge_\varepsilon v = u^4v^4 + c^5(u \times v) + (c^5t + t^3)(u \times v)^2 + c^5t^3(u \times v)^4,$$

$$u \wedge_{\varepsilon^*} v = u^4v^4 + t^5(u \times v) + (t^5t + c^3)(u \times v)^2 + t^5c^3(u \times v)^4.$$

Proof. We have $\varepsilon_6 = (a+1)t^2 = (c^5t^5)t^2 = c^5$; $\varepsilon_5 = at^3 = (c^5t^5 + 1)t^3 = c^5t + t^3$; $\varepsilon_3 = (a+1)t^5 = (c^5t^5)t^5 = c^5t^3$. Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Remark 4.12. The formulas to express parameters *are not necessarily unique*, because of dependences among parameters. For instance, we find $\varepsilon_5 = c^5t + t^3$, but also we can obtain

$$\varepsilon_5 = c^2t^5 + c^6t^2,$$

if we replace in $\varepsilon_5 = p^2q^2$, p and q by c^3t^6 and $c^5 + t^2$; but in fact we have effectively $c^2t^5 + c^6t^2 = c^5t + t^3$, which is equivalent to $(1+ < c, t >)c^5t = 0$. So the dependence $< c, t >= 1$ implies the equivalence of the two formulas for ε_5.

Proposition 4.13. 1 — The coefficients $\varepsilon_6, \varepsilon_5, \varepsilon_3$ in Proposition 4.11 and Proposition 4.5 are submitted to the following relations:

$$\mathrm{tr}\big((\varepsilon_3\varepsilon_6)^5\big) = 1.$$

$$\varepsilon_5 = \varepsilon_3^5\varepsilon_6^3 + \varepsilon_3\varepsilon_6^6.$$

2 — Conversely, given 2 parameters μ and ν, with $(\mu, \nu) \in \big(\mathbb{F}_8\big)^2\backslash\{0\}$, with

$$< \mu^5, \nu^5 >= 1, \quad \text{or equivalently} \quad \mu\nu \in \{1, R', S', I'\},$$

then a unique unordered basis ε is determined by (μ, ν), via its conjunction $\wedge_\varepsilon$ by

$$\varepsilon_6 = \mu, \quad \varepsilon_3 = \nu, \quad \varepsilon_5 = \nu^5\mu^3 + \nu\mu^6,$$

or equivalently by

$$t = \mu^2\nu^5, \quad c = \mu^3.$$

Proof. From Proposition 4.11 we have $\varepsilon_3\varepsilon_6 = c^5(c^5t^3) = c^3t^3 = (ct)^3$ i.e.

$$ct = (\varepsilon_3\varepsilon_6)^5;$$

and the condition $\mathrm{tr}(ct) = 1$ from Proposition 3.18 gives $\mathrm{tr}\big((\varepsilon_3\varepsilon_6)^5\big) = 1$.
For ε_5 we have $\frac{\varepsilon_3}{\varepsilon_6} = t^3$, $t = \big(\frac{\varepsilon_3}{\varepsilon_6}\big)^5$. We have $\varepsilon_5 = at^3 = (a+1)t^3+t^3 = (a+1)t^2t+t^3 = \varepsilon_6\big(\frac{\varepsilon_3}{\varepsilon_6}\big)^5 + \frac{\varepsilon_3}{\varepsilon_6}$, $\varepsilon_5 = \varepsilon_3^5\varepsilon_6^3 + \varepsilon_3\varepsilon_6^6$.
In the other direction from μ and ν we obtain of course ε_6 and ε_3, and then $c = \mu^3$, $ct = (\mu\nu)^5$, and then $t = \mu^2\nu^5$. Q.E.D.

4.2 The canonical parameters ρ, σ, ι, the differential parameters d_6, d_5, d_3

Here we introduce (ρ, σ, ι) and (d_6, d_5, d_3), two other parameters for a basis which are defined explicitly from the associated conjunction, and we express them with respect to the independent parameters (t, a) or the dual parameters (t, c). This will help us to provide explicit parametrizations of the conjunctions by (t, a) or (t, c). In the next sections, we will use the differential parameters d_6, d_5, d_3 as natural linear representations of conjunctions, to observe linear combinations of these operators. In fact by the intermediary of the parameters ρ, σ, ι the d_6, d_5, d_3 are directly accessible, and we can determine immediately the $\varepsilon_6, \varepsilon_5, \varepsilon_3$, from the data of the function $(u, v) \mapsto u \wedge_\varepsilon v$.

Definition 4.14. Given a basis ε and the associated conjunction $\wedge_\varepsilon$, we define its *κ-parameters* or *canonical parameters* as being

$$\rho = S \wedge_\varepsilon I, \quad \sigma = I \wedge_\varepsilon R, \quad \iota = R \wedge_\varepsilon S.$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 4.15. The canonical matrix K_ε from Proposition 4.7 is

$$K_\varepsilon = \begin{bmatrix} R & \iota & \sigma \\ \iota & S & \rho \\ \sigma & \rho & I \end{bmatrix}.$$

Proposition 4.16. Let ε be a basis, given by its matrix $M_\varepsilon = (m_{i,j})$, and the dual basis ε^* given by $M_{\varepsilon^*} =: (m^*_{i,j})$. Then the canonical parameters are given by

$$\begin{bmatrix} \rho \\ \sigma \\ \iota \end{bmatrix} = \begin{bmatrix} m^*_{2,1}m^*_{3,1} & m^*_{2,2}m^*_{3,2} & m^*_{2,3}m^*_{3,3} \\ m^*_{3,1}m^*_{1,1} & m^*_{3,2}m^*_{1,2} & m^*_{3,3}m^*_{1,3} \\ m^*_{1,1}m^*_{2,1} & m^*_{1,2}m^*_{2,2} & m^*_{1,3}m^*_{2,3} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}$$

Proof. The identity $M^{\mathrm{T}}_{\varepsilon^*} M_\varepsilon = I_3$ is given in Definition 3.5. For any u we have $\mathrm{Coord}_\varepsilon(u) = M_\varepsilon^{-1}\mathrm{Coord}_\kappa(u)$, and in particular $\mathrm{Coord}_\varepsilon(R)$, $\mathrm{Coord}_\varepsilon(S)$ and $\mathrm{Coord}_\varepsilon(I)$ are the columns of M_ε^{-1} (i.e. the rows of M_{ε^*}). Hence we have

$$S \wedge_\varepsilon I = (m^*_{2,1}m^*_{3,1})e_1 + (m^*_{2,2}m^*_{3,2})e_2 + (m^*_{2,3}m^*_{3,3})e_3.$$

Q.E.D.

Proposition 4.17. For a basis ε, if $(-)_i$ is the ith component with respect to $\kappa = (R, S, I)$, and with the canonical parameters given in Definition 4.14 and Proposition 4.16, we have

$$u \wedge_\varepsilon u' = u \wedge u' + (u \times u')_1\rho + (u \times u')_2\sigma + (u \times u')_3\iota.$$

Proof. For $u = xR+yS+zI$ and $u' = x'R+y'S+z'I$, we expand $u\wedge_\varepsilon u' = xx'R\wedge_\varepsilon R+xy'R\wedge_\varepsilon S+\cdots = xx'R + xy'\iota + \cdots = xx'R + yy'S + zz'I + (xy' + x'y)\iota + (yz' + y'z)\rho + (zx' + z'x)\sigma$, and as $xy' + x'y = (u \times u')_3$, etc., we arrive to the given formula. Q.E.D.

Proposition 4.18. With the notations of Definition 4.14 we have

$$W := \begin{bmatrix} \rho \\ \sigma \\ \iota \end{bmatrix} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix} \begin{bmatrix} \varepsilon_6 \\ \varepsilon_5 \\ \varepsilon_3 \end{bmatrix} + \begin{bmatrix} I' \\ R' \\ S' \end{bmatrix}.$$

$$E := \begin{bmatrix} \varepsilon_6 \\ \varepsilon_5 \\ \varepsilon_3 \end{bmatrix} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix} \begin{bmatrix} \rho \\ \sigma \\ \iota \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Proof. The first formula is a simple application of Proposition 4.5: we have $S \wedge_\varepsilon I = S^4I^4 + \varepsilon_6(S \times I) + \varepsilon_5(S \times I)^2 + \varepsilon_3(S \times I)^4 = I' + \varepsilon_6R + \varepsilon_5S + \varepsilon_3I$, etc. In fact the matrix $C_{RSI} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix}$, already present in Propositions 3.7 and 4.7, is its own inverse, $C^2_{RSI} = I_3$, hence the second formula. Another proof can be performed with $L_\varepsilon = C_{RSI}K_\varepsilon C_{RSI}$ from Proposition 4.7. Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Definition 4.19. For a given basis ε with *polynomial parameters* ε_6, ε_5 and ε_3 we define its *polynomial differential parameters* or briefly *differential parameters*:

$$d_6 = \varepsilon_6 + 1, \quad d_5 = \varepsilon_5, \quad d_3 = \varepsilon_3 + 1,$$

and

$$D_\varepsilon = \begin{bmatrix} 0 & d_3 & d_5 \\ d_3 & 0 & d_6 \\ d_5 & d_6 & 0 \end{bmatrix}.$$

These parameters are named 'differential' because they appear in the difference $\wedge - \wedge_\varepsilon$ as follows.

Proposition 4.20. With the notations of Definition 4.19 we have

$$\begin{bmatrix} d_6 \\ d_5 \\ d_3 \end{bmatrix} = \begin{bmatrix} R & S & I \\ S & I & R \\ I & R & S \end{bmatrix} \begin{bmatrix} \rho \\ \sigma \\ \iota \end{bmatrix} = C_{RSI} W.$$

Furthermore $u \wedge_\varepsilon v$ is given by

$$u \wedge_\varepsilon v = u \wedge v + d_6(u \times v) + d_5(u \times v)^2 + d_3(u \times v)^4.$$

Proof. The first formula is clear. For the second formula, we have two proofs. On the one hand, it is a trivial application of the definition of the d_6, d_5, d_3 with the formula in Proposition 4.5 for $u \wedge_\varepsilon v$ and the formula in Proposition 2.8 for $u \wedge v$. On the other hand we can use Proposition 4.17. As $(u \times u')_1 = \mathrm{tr}((u \times u')R) = (u \times u')R + (u \times u')^2 S + (u \times u')^4 I$, we find $u \wedge_\varepsilon u' = u \wedge u' + (R\rho + S\sigma + I\iota)(u \times u') + \cdots = u \wedge u' + d_6(u \times u') + \ldots$ Q.E.D.

Proposition 4.21. For the 4 auto-dual bases, the canonical parameters, the differential parameters and the polynomial parameters are:

ε	κ	r	s	i
ρ	0	1	I	S
σ	0	I	1	R
ι	0	S	R	1
d_6	0	R	S	I
d_5	0	S'	I'	R'
d_3	0	S'	I'	R'
ε_6	0	S'	I'	R'
ε_5	0	S'	I'	R'
ε_3	0	R	S	I

Proof. We do a direct verification. For example for $r = (R', I', 1)$ we have $S = I' + 1, R = R' + I' + 1, I = R' + 1$, hence $\rho = S \wedge_r I = 1$, $\sigma = I \wedge_r R = R' + 1 = I$, $\iota = R \wedge_r S = I' + 1 = S$. Then we obtain $d_6 = R\rho + S\sigma + I\iota = R$, $d_5 = S\rho + I\sigma + R\iota = S'$, $d_3 = I\rho + R\sigma + S\iota = S'$. An we finish with $\varepsilon_6 = d_6 + 1 = R + 1 = S'$, $\varepsilon_5 = d_5 = S'$, $\varepsilon_3 = d_3 + 1 = S' + 1 = R$. Q.E.D.

4.3 Differential parameters in terms of true and co-true

Proposition 4.22. The differential parameters d_6, d_5, d_3 introduced in 4.19 are given, with respect to t and c by:

$$d_6 = c^5 + 1, \quad d_5 = c^5 t + t^3, \quad d_3 = c^5 t^3 + 1.$$

Proof. It results from the expression of $\varepsilon_6, \varepsilon_5, \varepsilon_3$ given in Proposition 4.11. Q.E.D.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

5 The 28 logics given by their conjunctions

Now, with the help of the previous parametrizations, we are ready to produce tables and formulas for the 28 conjunctions present in the situation.

5.1 Description by polynomial parameters $\varepsilon_6, \varepsilon_5, \varepsilon_3$

Proposition 5.1. The 4 logics associated to κ, r, s and i are given by the negations

$$\neg_\kappa u = u + 1, \quad \neg_r u = u + R, \quad \neg_s u = u + S, \quad \neg_i u = u + I,$$

and the conjunctions:

$$u \wedge_\kappa v = u^4v^4 + 1(u^2v^4 + u^4v^2) + 0(uv^4 + u^4v) + 1(uv^2 + u^2v),$$
$$u \wedge_r v = u^4v^4 + S'(u^2v^4 + u^4v^2) + S'(uv^4 + u^4v) + R(uv^2 + u^2v),$$
$$u \wedge_s v = u^4v^4 + I'(u^2v^4 + u^4v^2) + I'(uv^4 + u^4v) + S(uv^2 + u^2v).$$
$$u \wedge_i v = u^4v^4 + R'(u^2v^4 + u^4v^2) + R'(uv^4 + u^4v) + I(uv^2 + u^2v).$$

Proof. For a basis $\varepsilon = (e_1, e_2, e_3)$, the corresponding (t, a) as in Proposition 3.12 are denoted by t_ε and a_ε. With $t_\varepsilon = e_1 + e_2 + e_3$, we have

$$t_\kappa = 1, t_r = R, t_s = S, t_i = I;$$

with $q_\varepsilon = e_1e_2 + e_2e_3 + e_3e_1$, we have $q_\kappa = 0, q_r = I, q_s = R, q_i = S$, and, with $a_\varepsilon = \frac{q_\varepsilon}{t_\varepsilon{}^2}$, we obtain

$$a_\kappa = 0, a_r = S, a_s = I, a_i = R;$$

then, by Proposition 4.10, we obtain the announced values for the coefficients. We can also use directly Proposition 4.5. We can also use Proposition 4.21. Q.E.D.

Proposition 5.2. In parallel with the table of the 28 bases in Proposition 3.13, we have the following table for the values of *polynomial coordinates* of the 28 conjunctions $\wedge_\varepsilon$ associated to the $28 = 7 \times 4$ values of (t, a), as defined in Proposition 4.4, and given by Proposition 4.10:

$$(\varepsilon_6, \varepsilon_5, \varepsilon_3) = ((a + 1)t^2, at^3, (a + 1)t^5) :$$

	$a = 0$	$a = R$	$a = S$	$a = I$
$t = 1$	$\wedge_\kappa = (\mathbf{1}, \mathbf{0}, \mathbf{1})$	$\wedge_{I'i} = (S', R, S')$	$\wedge_{R'r} = (I', S, I')$	$\wedge_{S's} = (R', I, R')$
$t = R$	$\wedge_{R\kappa} = (S, 0, S')$	$\wedge_{Ii} = (1, I, I')$	$\wedge_{\mathbf{r}} = (\mathbf{S}', \mathbf{S}', \mathbf{R})$	$\wedge_{R's} = (R, 1, I)$
$t = S$	$\wedge_{S\kappa} = (I, 0, I')$	$\wedge_{S'i} = (S, 1, R)$	$\wedge_{Rr} = (1, R, R')$	$\wedge_{\mathbf{s}} = (\mathbf{I}', \mathbf{I}', \mathbf{S})$
$t = I$	$\wedge_{I\kappa} = (R, 0, R')$	$\wedge_{\mathbf{i}} = (\mathbf{R}', \mathbf{R}', \mathbf{I})$	$\wedge_{I'r} = (I, 1, S)$	$\wedge_{Ss} = (1, S, S')$
$t = R'$	$\wedge_{R'\kappa} = (S', 0, S)$	$\wedge_{Si} = (I', S', 1)$	$\wedge_{S'r} = (R, R', S')$	$\wedge_{Is} = (I, R, R)$
$t = S'$	$\wedge_{S'\kappa} = (I', 0, I)$	$\wedge_{Ri} = (R, S, S)$	$\wedge_{Ir} = (R', I', 1)$	$\wedge_{I's} = (S, S', I')$
$t = I'$	$\wedge_{I'\kappa} = (R', 0, R)$	$\wedge_{R'i} = (I, I', R')$	$\wedge_{Sr} = (S, I, I)$	$\wedge_{Rs} = (S', R', 1)$

The logic associated to a basis ε is determined by its conjunction $\wedge_\varepsilon$.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proof. To obtain the table, we apply Proposition 4.10. Then we have to prove that so the logic is determined, and the unordered basis is determined too.
It is known that the set of logical functions associated to the Boolean algebraic structure given by ε could be obtained by compositions of its $\mathrm{NAND}_\varepsilon$ function which is $\mathrm{NAND}_\varepsilon(u,v) = \neg_\varepsilon(u \wedge_\varepsilon v)$. As $\neg_\varepsilon u = u + t_\varepsilon$, the question is to determine $t_\varepsilon = t$ from $(\varepsilon_6, \varepsilon_5, \varepsilon_3)$. As $a \in \{0, R, S, I\}$, $a \neq 1$, and $\varepsilon_6 \neq 0$, and $t^3 = \frac{\varepsilon_3}{\varepsilon_6}$ and $t = \left(\frac{\varepsilon_3}{\varepsilon_6}\right)^5 = \varepsilon_3^5\varepsilon_6^2$. Another proof is to realize that ε is constituted by the 3 atoms e_1, e_2, e_3 which determine the logic, and these are the roots of $X^3 + tX^2 + qX + p = 0$, and t, q and p are determined by $(\varepsilon_6, \varepsilon_5, \varepsilon_3)$; we find $t = \varepsilon_3^5\varepsilon_6^2$, $a = \varepsilon_5 t^4 = \varepsilon_3^6\varepsilon_5\varepsilon_6$, $q = \varepsilon_3^2\varepsilon_5\varepsilon_6^5$, $p = \varepsilon_3^6\varepsilon_5^2\varepsilon_6 + \varepsilon_3\varepsilon_6^6$.
So in order to determine t_ε and then the basis ε we just have to determine the coefficients ε_6, ε_5 and ε_3, as given in the table. Starting with $u \wedge_\varepsilon v$, we have $\iota = R \wedge_\varepsilon S$, $\rho = S \wedge_\varepsilon I$, $\sigma = I \wedge_\varepsilon R$, and ε_6, ε_5, ε_3 are given by Proposition 4.18. By a simple inspection we verify that $\mu\nu \in \{1, R', S', I'\}$. Q.E.D.

5.2 Description by differential parameters d_6, d_5, d_3

Proposition 5.3. The table of the 28 conjunctions according to the values of the *differential parameters* $(d_6, d_5, d_3) = (\varepsilon_6 + 1, \varepsilon_5, \varepsilon_3 + 1)$ is:

	$a = 0$	$a = R$	$a = S$	$a = I$
$t = 1$	$\wedge_\kappa = (\mathbf{0}, \mathbf{0}, \mathbf{0})$	$\wedge_{I'i} = (R, R, R)$	$\wedge_{R'r} = (S, S, S)$	$\wedge_{S's} = (I, I, I)$
$t = R$	$\wedge_{R\kappa} = (I', 0, R)$	$\wedge_{Ii} = (0, I, S)$	$\wedge_{\mathbf{r}} = (\mathbf{R}, \mathbf{S}', \mathbf{S}')$	$\wedge_{R's} = (S', 1, R')$
$t = S$	$\wedge_{S\kappa} = (R', 0, S)$	$\wedge_{S'i} = (I', 1, S')$	$\wedge_{Rr} = (0, R, I)$	$\wedge_{\mathbf{s}} = (\mathbf{S}, \mathbf{I}', \mathbf{I}')$
$t = I$	$\wedge_{I\kappa} = (S', 0, I)$	$\wedge_{\mathbf{i}} = (\mathbf{I}, \mathbf{R}', \mathbf{R}')$	$\wedge_{I'r} = (R', 1, I')$	$\wedge_{Ss} = (0, S, R)$
$t = R'$	$\wedge_{R'\kappa} = (R, 0, I')$	$\wedge_{Si} = (S, S', 0)$	$\wedge_{S'r} = (S', R', R)$	$\wedge_{Is} = (R', R, S')$
$t = S'$	$\wedge_{S'\kappa} = (S, 0, R')$	$\wedge_{Ri} = (S', S, I')$	$\wedge_{Ir} = (I, I', 0)$	$\wedge_{I's} = (I', S', S)$
$t = I'$	$\wedge_{I'\kappa} = (I, 0, S')$	$\wedge_{R'i} = (R', I', I)$	$\wedge_{Sr} = (I', I, R')$	$\wedge_{Rs} = (R, R', 0)$

Remark 5.4. We let the reader write the corresponding table with respect to (ρ, σ, ι), which is linearly dependent of (d_6, d_5, d_3), according to $W = CD$.

Proposition 5.5. Given a basis ε, with differential parameters d_6, d_5, d_3 we have, with $u \times v = \big(uv(u+v)\big)^2$,

$$u \wedge_\varepsilon v = u \wedge v + d_6(u \times v) + d_5(u \times v)^2 + d_3(u \times v)^4,$$

$$u \wedge_\varepsilon v = u \wedge v + (c^5 + 1)(u \times v) + (c^5 t + t^3)(u \times v)^2 + (c^5 t^3 + 1)(u \times v)^4.$$

Proof. It is immediate, using the formulas for $\wedge$ (Proposition 2.8), for $\wedge_\varepsilon$ (Proposition 4.5), the definition of d_6, d_5, d_3 (Definition 4.19) and Proposition 4.22. Q.E.D.

Remark 5.6. 1 — Looking to the formula for $\wedge_\varepsilon$ in Proposition 5.5, we notice the 'symmetry', denoted by $(-)^*$, which is the exchange of t and c, and this transforms $\wedge_\varepsilon$ into $\wedge_{\varepsilon^*}$.
2 — The parameters d_6, d_5, d_3 are dependent, the relations between them being the immediate transcription of the dependences between the $\varepsilon_6, \varepsilon_5, \varepsilon_3$, as in Proposition 4.13.

6 Multilogical construction of $\mathbb{P}(8)$, as a Boolean manifold

Now, with our parametric formulas and tables, we are ready to explore the space of Boolean conjunctions on $\mathbb{F}_8$.
As a simple example, by immediate inspection of the tables, we find linear relations:

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 6.1. Among the differential parameters we have:

$$\wedge_{R'\kappa} + \wedge_{S'\kappa} + \wedge_{I'\kappa} = \wedge_r + \wedge_s + \wedge_i = \wedge_{Ir} + \wedge_{Rs} + \wedge_{Si} = (1,0,0);$$

$$\wedge_{Sr} + \wedge_{Is} + \wedge_{Ri} = \wedge_{I'r} + \wedge_{R's} + \wedge_{S'i} = (0,1,0);$$

$$\wedge_{R\kappa} + \wedge_{S\kappa} + \wedge_{I\kappa} = \wedge_{S'r} + \wedge_{I's} + \wedge_{R'i} = (0,0,1),$$

$$\wedge_{R'r} + \wedge_{S's} + \wedge_{I'i} = (1,1,1),$$

$$\wedge_{Rr} + \wedge_{Ss} + \wedge_{Ii} = (0,1,1).$$

Now we have to prove that, by compositions, 4 of the conjunctions generate completely $\mathbb{P}(8)$.

Proposition 6.2. We have the following identities:

$$uv = (u \wedge v)^2 + (u \times v) + (u \times v)^2,$$

$$u \times v = u \wedge_\kappa v + u \wedge_r v + u \wedge_s v + u \wedge_i v,$$

$$u^2 = R \times (S \times u) + S \times (I \times u) + I \times (R \times u).$$

Proof. We know that $u \wedge v = u^4 v^4 + (u \times v) + (u \times v)^4$, we derive $(u \wedge v)^2 = uv + (u \times v)^2 + (u \times v)$, the announced formula. So we only need formulas for $u \times v$ and u^2. For $u \times v$ we add the last 4 lines in Proposition 5.1. And for u^2 we have the following calculus. By the double cross product formula given in Proposition 3.2 which is $u \times (u' \times u'') =< u, u'' > u' + < u, u' > u''$, we deduce $R \times (S \times u) =< R, u > S$, $S \times (I \times u) =< S, u > I$, $I \times (R \times u) =< I, u > R$, and so the announced formula, by summing the three terms. Q.E.D.

Remark 6.3. Of course the formulas are not at all unique. For example the formula given for $u \times v$ could be modified with the help of Proposition 6.1.

Proposition 6.4. 1 — If A, B, C are the generators of $\mathrm{GL}_3(\mathbb{F}_2)$ presented in Proposition 2.6, we have

$$\wedge_A = \wedge_{R'i}, \quad \wedge_B = \wedge_{S'r}, \quad \wedge_C = \wedge_{I's}; \quad \wedge_{A^*} = \wedge_{Ri}, \quad \wedge_{B^*} = \wedge_{Sr}, \quad \wedge_{C*} = \wedge_{Is}.$$

2 — Furthermore we have

$$(u \times v)^2 = u \wedge_\kappa v + u \wedge_{A^*} v + u \wedge_{B^*} + u \wedge_{C^*} v,$$

$$(u \times v)^4 = u \wedge_\kappa v + u \wedge_A v + u \wedge_B + u \wedge_C v.$$

Proof. Except for the order of terms, A is $R'i$, B is $S'r$, C is $I's$, and the dual bases are A^* which is Ri, B^* which is Sr, C^* which is Is. We conclude with Proposition 6.1. Q.E.D.

Other formulas are possible for u^2, u^4, $\mathrm{tr}(u)$. In the next Proposition 6.5 we see how to obtain $(-)^2$ from the linear generators. But after that we will have to obtain a description of $(-)^2$ from the unique data of logical operators (Propositions 6.6 and 6.7).

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Proposition 6.5. Using A, B, C the generators of $\mathrm{GL}_3(\mathbb{F}_2)$ given in Proposition 2.6 we have:

$$\underline{A}(u) = R \times (S \times u) + u,\ \underline{B}(u) = S \times (I \times u) + u,\ \underline{C}(u) = I \times (R \times u) + u,$$

$$u^2 = \underline{A}(u) + \underline{B}(u) + \underline{C}(u) + u.$$

Using $r = ACB, s = BAC, i = CBA$, the three other generators given in Proposition 2.6, we have

$$u^2 = \underline{r}(u) + \underline{s}(u) + \underline{i}(u).$$

Proof. For the generators A, B, C in Proposition 6.2 we have computed $R \times (S \times u) =< R, u > S = (Ru + R^2u^2 + R^4u^4)S = R'u^4 + Iu^2 + I'u$, and we have $\underline{A}(u) = R'u^4 + Iu^2 + Su$ (see example in 'Convention' in section 2.3). For the formula with r, s, i we have (see 'Convention', in section 2.3) $\underline{r}(u) = R'u^4 + u^2 + I'u$. Q.E.D.

Proposition 6.6. We have

$$u = u \wedge_r R + u \wedge_s S + u \wedge_i I,$$

$$u^2 = u \wedge_r I + u \wedge_s R + u \wedge_i S,$$

$$u^4 = u \wedge_r S + u \wedge_s I + u \wedge_i R,$$

$$\mathrm{tr}(u) = u \wedge_r 1 = u \wedge_s 1 = u \wedge_i 1.$$

Proof. As $u \wedge_r v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_r [v]_{\mathrm{sq}}$, $u \wedge_s v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_s [v]_{\mathrm{sq}}$, $u \wedge_i v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_i [v]_{\mathrm{sq}}$, with the definition of L_ε from Proposition 4.6, and

$$L_r = \begin{bmatrix} 0 & R & S' \\ R & 0 & S' \\ S' & S' & 1 \end{bmatrix},\quad L_s = \begin{bmatrix} 0 & S & I' \\ S & 0 & I' \\ I' & I' & 1 \end{bmatrix},\quad L_i = \begin{bmatrix} 0 & I & R' \\ I & 0 & R' \\ R' & R' & 1 \end{bmatrix},$$

we obtain:

$$u \wedge_r R = u,\quad u \wedge_r S = Iu^4 + S'u^2 + I'u,\quad u \wedge_r I = R'u^4 + Ru^2 + I'u.$$

$$u \wedge_s R = S'u^4 + Su^2 + R'u,\quad u \wedge_s S = u,\quad u \wedge_s I = Ru^4 + I'u^2 + R'u,$$

$$u \wedge_i R = Su^4 + R'u^2 + S'u,,\quad u \wedge_i S = I'u^4 + Iu^2 + S'u,\quad u \wedge_i I = u.$$

Q.E.D.

Proposition 6.7. We have

$$u^2 = u \wedge_A 1 + u \wedge_B 1 + u \wedge_C 1,$$

$$u^4 = u \wedge_{A^*} 1 + u \wedge_{B^*} 1 + u \wedge_{C^*} 1.$$

Proof. We know that $u \wedge_A v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_A [v]_{\mathrm{sq}}$, $u \wedge_B v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_B [v]_{\mathrm{sq}}$, and that $u \wedge_C v = [u]_{\mathrm{sq}}{}^{\mathrm{T}} L_C [v]_{\mathrm{sq}}$, where, according to Proposition 6.4, we have, with the table in Proposition 5.2,

$$L_A = \begin{bmatrix} 0 & R' & I' \\ R' & 0 & I \\ I' & I & 1 \end{bmatrix},\quad L_B = \begin{bmatrix} 0 & S' & R' \\ S' & 0 & R \\ R' & R & 1 \end{bmatrix},\quad L_C = \begin{bmatrix} 0 & I' & S' \\ I' & 0 & S \\ S' & S & 1 \end{bmatrix}.$$

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

Then we obtain:

$$u \wedge_A 1 = S'u^4 + u^2 + S'u, u \wedge_B 1 = I'u^4 + u^2 + I'u, u \wedge_C 1 = R'u^4 + u^2 + R'u.$$

Similarly with

$$L_{A^*} = \begin{bmatrix} 0 & S & S \\ S & 0 & R \\ S & R & 1 \end{bmatrix}, \quad L_{B^*} = \begin{bmatrix} 0 & I & I \\ I & 0 & S \\ I & S & 1 \end{bmatrix}, \quad L_{C^*} = \begin{bmatrix} 0 & R & R \\ R & 0 & I \\ R & I & 1 \end{bmatrix},$$

we obtain

$$u \wedge_{A^*} 1 = Iu^4 + R'u^2, \quad u \wedge_{B^*} 1 = Ru^4 + S'u^2, \quad u \wedge_{A^*} 1 = Su^4 + I'u^2.$$

Q.E.D.

In [5] we proved that a construction is possible for the Post-Malcev algebra $\mathbb{P}(8)$ (cf. Definition 2.9) with $\wedge$, $\neg$ and the cross products $R^\times$, $S^\times$, $I^\times$. Now we have the following construction which is a logical counterpart of the structure of $\mathrm{GL}_3(\mathbb{F}_2)$. It depends on the generators r, s, i or A, B, C of $\mathrm{GL}_3(\mathbb{F}_2)$, and the ternary symmetry between them.

Proposition 6.8. 1 — The Post-Malcev algebra $\mathbb{P}(8)$ could be generated by compositions of the functions

$$\neg, \wedge, \wedge_r, \wedge_s, \wedge_i,$$

and the constant functions with values R, S and I.
So $\mathbb{P}(8)$ is generated by the union in $\mathbb{P}(8)$ of 4 subalgebras isomorphic to $\mathbb{P}_2$, namely $(\mathbb{P}(8))_\kappa$, $(\mathbb{P}(8))_r$, $(\mathbb{P}(8))_s$, $(\mathbb{P}(8))_i$, respectively generated by $\{\neg_\kappa, \wedge_\kappa\}$, $\{\neg_r, \wedge_r\}$, $\{\neg_s, \wedge_s\}$, $\{\neg_i, \wedge_i\}$.
2 — To generate $\mathbb{P}(8)$, rather than the $\wedge_r, \wedge_s, \wedge_i$ we can use the $\wedge_A, \wedge_B, \wedge_B$, or the $\wedge_{A^*}, \wedge_{B^*}, \wedge_{B^*}$.

Proof. The Post-Malcev algebra $\mathbb{P}(8)$ (cf. Definition 2.9) is constructible with polynomials over $\mathbb{F}_8$, because $\mathbb{F}_8$ is a finite field, and so we have to obtain the functions $u + v$ and uv. For $u + v$ we have

$$u + v = \neg\Big(\big(\neg(\neg u \wedge v)\big) \wedge \big(\neg(u \wedge \neg v)\big)\Big).$$

For uv we have the formula in Proposition 6.2, expressed with u^2 and $u \times v$, and the formulas for u^2 and $u \times v$. For u^2 we can use also Proposition 6.6.
For the second point we use Proposition 6.7 to generate $(-)^2$ or $(-)^4$, and then Proposition 6.4 to obtain $u \times v$, and finally Proposition 6.2 to obtain uv. Q.E.D.

References

[1] M. Andreatta, A. Ehresmann, R. Guitart and G. Mazzola, *Towards a categorical theory of creativity for music, discourse, and cognition*, in J. Yust, J. Wild, and J.A. Burgoyne (Eds.): MCM 2013, LNAI 7937, pp. 19-37, 2013, Springer.

[2] R. Guitart, *Moving logic, from Boole to Galois*, Colloque International "Charles Ehresmann : 100 ans", 7-9 october 2005, Amiens, Cahiers Top Géo Diff Cat. vol. XLVI-3, 2005, 196-198.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM

[3] R. Guitart, *Klein's group as a borromean object*, Cahiers Top. Géo. Diff. Cat. vol. L-2, 2009, 144-155.

[4] R. Guitart, *A Hexagonal framework of the field* $\mathbb{F}_4$ *and the associated Borromean logic*, Log. Univers.,6 (1-2), 2012, 119-147.

[5] R. Guitart, *Hexagonal logic of the field* $\mathbb{F}_8$ *as a boolean logic with three involutive modalities*, in A. Koslow, A. Buchsbaum (eds.), The Road to Universal Logic, Studies in Universal Logic, Birkhäuser, 2015. p. 191-220.

[6] D. Lau, *Function Algebras on finite sets*, Springer, 2006.

[7] H.W. Lenstra Jr. and R.J. Schoof, *Primitive normal basis for finite fields*, Math. Comp., 48, 1987, 217-231.

[8] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, C.U.P., 1994.

[9] A. I. Malcev, *Iterative algebra and Post's varieties* (Russian), Algebra i Logika (Sem.) 5, 1966, 5-24.

Brought to you by | UCL - University College London
Authenticated
Download Date | 3/22/19 4:15 PM