Moving Logic, from Boole to Galois *

René Guitart

If a group G acts on a set X and if $(\wedge_g, \neg_g)_{g\in G}$ is a family of boolean structures on X such that $gx \wedge_{gh} gy = g(x \wedge_h y)$ and $\neg_{gh} gx = g(\neg_h x)$, then we speak of a G-*moving boolean logic* or shortly of a G-moving logic. In fact every such datum is equivalent to the datum of the action of G on X and of one boolean structure $(\wedge, \neg)$ on X: then we recover $(\wedge_g, \neg_g)$ by $x \wedge_g y = g(g^{-1}x \wedge g^{-1}y)$ and $\neg_g x = g(\neg g^{-1}x)$.

If $V = (\wedge_i, \neg_i)_{i\in I}$ is a family of boolean structures on a set X then we say that a function $f : X^k \to X$ is a V-*moving boolean* function if f can be defined using constants in X, $\wedge_i$, $\neg_i$, with possibly various $i \in I$ occuring in it.

Theorem 1. *For every finite set X of cardinal 2^n with n odd (resp. even), there is a family V of 4 (resp. 3) boolean structures on X — different but isomorphic, and with the same 'false'= 0 and the same addition '+' — such that, for every integer k, every function $f : X^k \to X$ is a V-*moving boolean function.

As for *Specular Logic* [3], moving logics and moving functions can be used for *discourse analysis*. But here we just want to show how it links boolean and galoisian calculi, and how in this way Theorem 1 is proved.

For every integer n the set $2^n = \{0,1\}^n$ is equipped with a boolean structure and a field structure, $\mathbb{B}^n$ and $\mathbb{F}_{2^n}$, both unique up to isomorphisms. If the addition $+$ is fixed as being the same in $\mathbb{B}^n$ and in $\mathbb{F}_{2^n}$, then a natural question arises: what is the link between multiplication "$\times$" in $\mathbb{F}_{2^n}$ with zero 0 and unit 1 and conjonctions "$\wedge$" in $\mathbb{B}^n$ with 'false' = 0 and 'true' = t? In one direction, it is clear: if $\varphi = (e_1, \ldots, e_n)$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then we get a conjonction $\wedge_\varphi$ by $(\sum_1^n x_i \times e_i) \wedge_\varphi (\sum_i^n y_i \times e_i) = \sum_i^n x_i \times y_i \times e_i$, when for all $i \le n$, x_i and y_i are 0 or 1; and negation, disjunction and implication by $\neg_\varphi(x) = x + t_\varphi$, with $t_\varphi = \sum_1^n e_i$, $x \vee_\varphi y = \neg_\varphi(\neg_\varphi x \wedge_\varphi \neg_\varphi y)$, $x \Rightarrow_\varphi y = (\neg_\varphi x) \vee_\varphi y$. So we get a boolean structure Boole_φ associated with a basis φ, with false 0 and true t_φ, and of course the operations of Boole_φ, as every functions $f : \mathbb{F}_{2^n}^k \to \mathbb{F}_{2^n}$, can be expressed with $\times$ and $+$. In fact, the crucial point between boolean and galoisian calculi is that $x \wedge_\varphi x = x$, whereas $x \times x \neq x$, but $x \times x$ and x are *undiscernible*: $x^2 \sim x$; this is the meaning of the fact that the Frobenius map $x \mapsto x^2$ generates the Galois group of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. So, in order to go in the other direction — i.e. to come back from boolean structures to polynomial functions in a Galois field of characteristic 2 —

* *Colloque International "Charles Ehresmann : 100 ans"*, Amiens 7–9 octobre 2005, *Cahiers Top. Géo. Diff. Cat.*, vol. XLVI–3, 2005, p. 196–198.

our proposed method is first to get the product $\times$ with one boolean structure and the Frobenius, and then to get the Frobenius as a moving boolean function. We first do that for $n = 2, 3$ and show in these cases that *every function is moving boolean.*

In the case $n = 2$, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2{+}X{+}1)$. With u and v the two imaginary roots of X^2+X+1 over $\mathbb{F}_2$, $u \times v = 1$, $u + v = 1$, and $\mathbb{F}_4 = \{0, 1, u, v\}$. Ordered bases of $\mathbb{F}_4$ over $\mathbb{F}_2$ determine the group $\mathrm{GL}_2(\mathbb{F}_2) \simeq \mathcal{S}_3$, for which we consider spanning by $p = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $q = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which are, with respect to the basis $\kappa = (u, v)$ with $t_\kappa = 1$, the matrices of the basis $\alpha = (1, v)$ with $t_\alpha = u$, and $\beta = (u, 1)$ with $t_\beta = v$. So $p(x) = ux^2$ and $q(x) = vx^2$.

Theorem 2 [1]. *In $\mathbb{F}_4$ we have $x \wedge_\varphi y = x^2y^2 + t_\varphi(x^2y + xy^2)$, and in particular $x \wedge_\kappa y = x^2y^2 + x^2y + xy^2$. With $\wedge = \wedge_\kappa$, we have $x \times y = x^2 \wedge y + x \wedge y^2 + x^2 \wedge y^2$. Every fonction on $\mathbb{F}_4^k$ with values in $\mathbb{F}_4$ is a composition of constants, $\wedge$, $\neg$, and $(-)^2$. Furthermore, we have $p(x) + q(x) = x^2$, and every function is a composition of constants, $\wedge$, $\neg$, and p, q. As in fact $x^2 = x \wedge_\kappa 1 + x \wedge_\alpha 1 + x \wedge_\beta 1$, we get also that every function is a $\{\kappa, \alpha, \beta\}$-*moving boolean fonction.

We now consider the case $n = 3$, $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3{+}X^2{+}1)$. With a, b, c the three imaginary roots of $X^3 + X^2 + 1$ over $\mathbb{F}_2$, a^{-1}, b^{-1}, c^{-1} are the roots of $X^3 + X + 1$, $abc = 1$, $ab + bc + ca = 0$, $a + b + c = 1$, $a^{-1} = c + 1 = bc$, $b^{-1} = a + 1 = ca$, $c^{-1} = b + 1 = ab$, $a^2 = b$, $b^2 = c$, $c^2 = a$, $a + a^{-1} = b$, $b + b^{-1} = c$, $c + c^{-1} = a$, $\mathbb{F}_8 = \{0, 1, a, b, c, a^{-1}, b^{-1}, c^{-1}\}$. Ordered bases of $\mathbb{F}_8$ over $\mathbb{F}_2$ are organized as the simple group $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$, of order 168, which is the group of automorphisms of the Klein's quartic $\mathrm{X}(7) = \{[x : y : z] \in \mathrm{P}_2(\mathbb{C}); x^3y + y^3z + z^3x = 0\}$ (the most symmetric riemannian surface of genus 3). Now, in $\mathrm{GL}_3(\mathbb{F}_2)$ we consider the order-seven matrices $r = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$, $s = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, $i = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, which are, with respect to the unique normal basis $\kappa = (a, b, c)$, the matrices of the three other strictly auto-dual bases $\rho = (a^{-1}, c^{-1}, 1)$, $\sigma = (1, b^{-1}, a^{-1})$, $\iota = (b^{-1}, 1, c^{-1})$. So $r(x) = a^{-1}x^4 + x^2 + c^{-1}x$, $s(x) = b^{-1}x^4 + x^2 + a^{-1}x$, and $i(x) = c^{-1}x^4 + x^2 + b^{-1}x$.

The actions of r, s, i on $1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$, $\ldots$, $7 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, are the $7-$cycles $r = [1746325]$, $s = [1647235]$, $i = [1564327]$, with a visible ternary symetry (Fig. 1) realizable in $\mathcal{S}_7$ with $j = (142)(356) : jrj^{-1} = s$, $jsj^{-1} = i$, $jij^{-1} = r$.

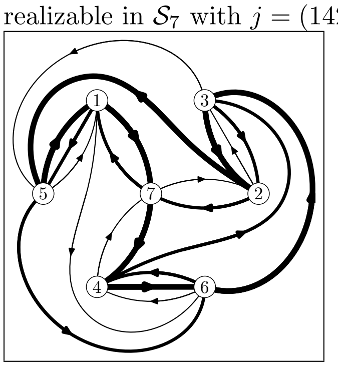

Figure 1: symetry of r, s, i

Theorem 3 [2]. $\mathrm{GL}_3(\mathbb{F}_2)$ *is generated by r, s and i with the relations $(srir^{-1})^2 = 1$, $(is^3i^{-1})^7 = 1$, $((is^3i^{-1})(srir^{-1}))^3 = 1$, $((is^3i^{-1})^4(srir^{-1}))^4 = 1$. And if $w(r, s, i) = 1$ is satisfied, with $w(r, s, i)$ any word in r, s, i, then also $w(s, i, r) = 1$, $w(i, r, s) = 1$; we speak here of a* borromean spanning *of* $\mathrm{GL}_3(\mathbb{F}_2)$.

Theorem 4. *For $\varphi = (f_1, f_2, f_3)$ a basis of $\mathbb{F}_8$ with matrix m we have $x \wedge_\varphi y = m(m^{-1}x \wedge_\kappa m^{-1}y)$, and if with $q = (f_1 + f_2 + f_3)(f_1f_2 + f_2f_3 + f_3f_1)(f_1f_2f_3)^{-1}$ we take $t = (q + 1)^4$, $\lambda = (f_1 + f_2 + f_3)t^{-1}$, $\mu = 1 + t^2 + t^3 + t^4 + t^5 + t^6 + t^7$, then we get $\neg_\varphi(x) = x + t$,*

$x \wedge_\varphi y = x^4y^4 + \lambda^{-5}\mu[x^4y^2 + x^2y^4] + +\lambda^{-4}(t+1)[x^4y + xy^4] + \lambda^{-2}t[x^2y + xy^2]$.
In particular we have $x \wedge_\kappa y = x^4y^4 + 1[x^4y^2 + x^2y^4] + 0[x^4y + xy^4] + 1[x^2y + xy^2]$,

$x \wedge_\rho y = x^4y^4 + (a+1)[x^4y^2 + x^2y^4] + (a+1)[x^4y + xy^4] + a[x^2y + xy^2]$, $t_\rho = a$,

$x \wedge_\sigma y = x^4y^4 + (b+1)[x^4y^2 + x^2y^4] + (b+1)[x^4y + xy^4] + b[x^2y + xy^2]$, $t_\sigma = b$,

$x \wedge_\iota y = x^4y^4 + (c+1)[x^4y^2 + x^2y^4] + (c+1)[x^4y + xy^4] + c[x^2y + xy^2]$, $t_\iota = c$.

Theorem 5. *As a kind of counterpart of the borromean spanning of* $\mathrm{GL}_3(\mathbb{F}_2)$ *we get on* $\mathbb{F}_8$ *a symetric system of six projectors 'by intersection', with associated logical expressions for* $x \mapsto x^4$ *and its inverse* $x \mapsto x^2$*:*

$x\wedge_\rho b = cx^4 + b^{-1}x^2 + c^{-1}x$, $x\wedge_\sigma c = ax^4 + c^{-1}x^2 + a^{-1}x$, $x\wedge_\iota a = bx^4 + a^{-1}x^2 + b^{-1}x$,

$x\wedge_\rho c = a^{-1}x^4 + ax^2 + c^{-1}x$, $x\wedge_\sigma a = b^{-1}x^4 + bx^2 + a^{-1}x$, $x\wedge_\iota b = c^{-1}x^4 + cx^2 + b^{-1}x$,

$x^4 = x\wedge_\rho b + x\wedge_\sigma c + x\wedge_\iota a$, $x^2 = x\wedge_\rho c + x\wedge_\sigma a + x\wedge_\iota b$.

Theorem 6. *In* $\mathbb{F}_8$*, with* $\wedge = \wedge_\kappa$*, the product is* $x \times y = x^2 \wedge y^2 + x \wedge y^4 + x^4 \wedge y + x^4 \wedge y^2 + x^2 \wedge y^4$*, and so every function on* $\mathbb{F}_8^k$ *with values in* $\mathbb{F}_8$ *is a composition of constants,* $\wedge$*,* $\neg$*, and* $(-)^2$*. Furthermore, we have* $r(x) + s(x) + i(x) = x^2$*, and every function is a composition of constants,* $\wedge$*,* $\neg$*,* r*,* s*,* i*. As* $x^2 = x\wedge_\rho c + x\wedge_\sigma a + x\wedge_\iota b$*, every function is also a* $\{\kappa, \rho, \sigma, \iota\}$-moving boolean function.

Now, we are ready for the general case (and then Theorem 1):

Theorem 7. *In* $\mathbb{F}_{2^n}$*, every function is a composition of constants,* $\wedge, \neg$ *and* $(-)^2$*, for* $(\wedge, \neg)$ *a boolean structure on* $\mathbb{F}_{2^n}$ *associated to a normal basis, and* $(-)^2$ *the Frobenius map. There is a subset* V *of* $\mathrm{GL}_n(\mathbb{F}_2)$ *— of cardinal* 4 *if* n *is odd, and* 3 *if* n *is even — such that for every integer* k*, every function* $\mathbb{F}_{2^n}^k \to \mathbb{F}_{2^n}$ *is a* V-moving boolean function.

The idea of the proof is inspired by the cases $n = 2, 3$. $\mathbb{F}_{2^n}$ is now equipped with a *normal* basis $\beta = (b_1, \ldots, b_n)$, with $b_i = (b_n)^{2^i}$. With some $\gamma_{i,j,k} \in \mathbb{F}_2$ (to be precised only for computing an explicit result, as we did for $n = 2, 3$), $(\sum_i x_i b_i) \times (\sum_j x_i b_j) = \sum_{i,j,k} \gamma_{i,j,k} x_i y_j b_k$. We get for example $(x \wedge_\beta y^{2^m})^{2^l} \wedge_\beta b_{i+l} = x_i y_{i-m} b_{i+l}$. The general operator $x \mapsto y \wedge_\varphi z$, for an arbitrary basis φ with matrix A with respect to β and an arbitrary z can be written as $x \mapsto A(A^{-1}z)^d A^{-1}x$ (with $(A^{-1}z)^d$ the diagonal matrix given by $((A^{-1}z)^d)_{i,i} = (A^{-1}z)_i$) and is the general projector $x \mapsto Px$, with P linear and $P^2 = P$. And here, in the context of $\mathbb{F}_2$, every linear map is a sum of projectors; in particular with π_i the matrix with 1 at (i,i) and $(i+1, i)$, for $i < n$, and π_n the matrix with 1 at (n,n) and $(1,n)$, we get $x^2 = x + (\sum_{(i<n)\,\&\,(i\,\mathrm{odd})} \pi_i) + (\sum_{(i\leq n)\,\&\,(i\,\mathrm{even})} \pi_i) + (\pi_n)\,\&\,(n\,\mathrm{odd})$.

[1] *Théorie cohomologique du sens*, SIC, 8 nov. 2003, compte-rendu, 2004-10/Mars 2004, LAMFA-CNRS UMR 6140, 39-47 [version allongée le 9 février 2004, 22 p].

[2] *Borroméanité du groupe* G_{168} *de la quartique de Klein*, en préparation, 2005.

[3] L'idée de Logique Spéculaire, *Journées Mathématiques Catégories, Algèbres, Esquisses et Néo-esquisses (C.A.E.N.)*, Univ. de Caen, 27-30 septembre 1994, 127-132.