Moving Logic, from Boole to Galois *

René Guitart

If a group $G$ acts on a set $X$ and if $(\land_g, \neg_g)_{g \in G}$ is a family of boolean structures on $X$ such that $gx \land_{gh} gy = g(x \land_h y)$ 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 $(\land, \neg)$ on $X$: then we recover $(\land_g, \neg_g)$ by $x \land_y y = g(g^{-1}x \land g^{-1}y)$ and $\neg_gx = g(\neg^{-1}x)$.

If $V = (\land_i, \neg_i)_{i \in I}$ is a family of boolean structures on a set $X$ then we say that a function $f : X^k \rightarrow X$ is a $V$-moving boolean function if $f$ can be defined using constants in $X$, $\land_i$, $\neg_i$, with possibly various $i \in I$ occurring 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 $f : X^k \rightarrow X$ 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 “$x$” in $\mathbb{F}_2^n$ with zero 0 and unit 1 and conjunctions “$\land$” 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 conjunction $\land_{\varphi}$ by $(\sum_i^n x_i \times e_i) \land_{\varphi} (\sum_i^n y_i \times e_i) = \sum_i^n x_i \times y_i \times e_i$, when for all $i \leq n$, $x_i$ and $y_i$ are 0 or 1; and negation, disjunction and implication by $\neg_{\varphi}(x) = x + t_{\varphi}$, with $t_{\varphi} = \sum_i^n e_i$, $x \lor_{\varphi} y = \neg_{\varphi}(\neg_{\varphi}x \land_{\varphi} \neg_{\varphi}y)$, $x \Rightarrow_{\varphi} y = (\neg_{\varphi}x) \lor_{\varphi} y$. So we get a boolean structure $\text{Boole}_{\varphi}$ associated with a basis $\varphi$, with false 0 and true $t_{\varphi}$, and of course the operations of $\text{Boole}_{\varphi}$, as every functions $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, can be expressed with $\times$ and $\lor$. In fact, the crucial point between boolean and galoisian calculi is that $x \land_{\varphi} x = x$, whereas $x \times x \neq x$, but $x \times x$ and $x$ are indiscernible: $x^2 \sim x$; 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 —

---

our proposed method is first to get the product $x$ 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 $n = 2$, $F_4 = F_2[X]/(X^2 + X + 1)$. With $u$ and $v$ the two imaginary roots of $X^2 + X + 1$ over $F_2$, $u + v = 1$, $u + v = 1$, and $F_4 = \{0, 1, u, v\}$. Ordered bases of $F_4$ over $F_2$ determine the group $GL_2(F_2) \simeq S_3$, for which we consider spanning by $p = \left[ \begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix} \right]$, $q = \left[ \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right]$, 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 $F_4$ we have $x \land \varphi y = x^2y^2 + t_\varphi(x^2y + xy^2)$, and in particular $x \land \kappa y = x^2y^2 + x^2y + xy^2$. With $\land = \land_\kappa$, we have $x \land y = x^2 \land y + x \land y^2 + x^2 \land y^2$. Every function on $F_4$ with values in $F_4$ is a composition of constants, $\land, \land, \land$, and $(-)^2$. Furthermore, we have $p(x) + q(x) = x^2$, and every function is a composition of constants, $\land, \land, \land$, and $p, q$. As in fact $x^2 = x \land_\kappa 1 + x \land_\kappa 1 + x \land_\kappa 1$, we get also that every function is a $\{\kappa, \alpha, \beta\}$-moving boolean function.

We now consider the case $n = 3$, $F_8 = F_2[X]/(X^3 + X^2 + 1)$. With $a, b, c$ the three imaginary roots of $X^3 + X^2 + 1$ over $F_2$, $a^{-1}, b^{-1}, c^{-1}$ are the roots of $X^3 + X + 1$, $abc = 1$, $ab + bc + ca = 0$, $a + b + c = 1$, $a^{-1} = c + 1 = bc$, $b^{-1} = a + 1 = ca$, $c^{-1} = b + 1 = ab$, $a^2 = b$, $b^2 = c$, $c^2 = a$, $a + a^{-1} = b$, $b + b^{-1} = c$, $c + c^{-1} = a$, $F_8 = \{0, 1, a, b, c, a^{-1}, b^{-1}, c^{-1}\}$. Ordered bases of $F_8$ over $F_2$ are organized as the simple group $GL_3(F_2) \simeq PSL_2(F_7)$, of order 168, which is the group of automorphisms of the Klein’s quartic $X(7) = \{[x : y : z] \in P_2(\mathbb{C}) : x^3y + y^3z + z^3x = 0\}$ (the most symmetric riemannian surface of genus 3). Now, in $GL_3(F_2)$ we consider the ordered seven matrices $r = \left[ \begin{smallmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix} \right]$, $s = \left[ \begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{smallmatrix} \right]$, $i = \left[ \begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{smallmatrix} \right]$, 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 $1 = \left[ \begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix} \right]$, $2 = \left[ \begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix} \right]$, ..., $7 = \left[ \begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix} \right]$, are the 7-cycles $r = [1746325]$, $s = [1647235]$, $i = [1564327]$, with a visible ternary symmetry (Fig. 1) realizable in $S_7$ with $j = (142)(356)$ : $jrj^{-1} = s$, $jsj^{-1} = i$, $jit^{-1} = r$.

**Theorem 3 [2].** $GL_3(F_2)$ is generated by $r, s$ and $i$ with the relations $(sr) = 1$, $(is^3) = 1$, $((is^3)^{i})(isr)^{-4} = 1$, and $(is^3)^{-4}(sr)^{-4} = 1$. 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 $GL_3(F_2)$.

**Theorem 4.** For $\varphi = (f_1, f_2, f_3)$ a basis of $F_8$ with matrix $m$ we have $x \land \varphi y = m(m^{-1}x \land \kappa m^{-1}y)$, and if with $q = (f_1 + f_2 + f_3)(f_1f_2 + f_2f_3 + f_3f_1)(f_1f_2f_3)$ we take $t = (q + 1)^4$, $\lambda = (f_1 + f_2 + f_3)^{-4}$, $\mu = 1 + t^5 + t^4 + t^3 + t^2 + t^2$, then we get $\neg \varphi(x) = x + t$. 

---

**Figure 1:** symmetry of $r, s, i$
$x \land \varphi y = x^4 y^4 + \lambda^{-5} \mu [x^4 y^2 + x^2 y^4] + \lambda^{-4} (t + 1) [x^4 y + xy^4] + \lambda^{-2} t [x^2 y + xy^2].$

In particular we have $x \land \alpha y = x^4 y^4 + 1 [x^4 y^2 + x^2 y^4] + 0 [x^3 y + xy^3] + 1 [x^2 y + xy^2],$ $x \land \rho y = x^4 y^4 + (a + 1) [x^4 y^2 + x^2 y^4] + (a + 1) [x^4 y + xy^4] + a [x^2 y + xy^2],$ $t_\rho = a,$ $x \land \gamma y = x^4 y^4 + (b + 1) [x^4 y^2 + x^2 y^4] + (b + 1) [x^4 y + xy^4] + b [x^2 y + xy^2],$ $t_\sigma = b,$ $x \land \varsigma y = x^4 y^4 + (c + 1) [x^4 y^2 + x^2 y^4] + (c + 1) [x^4 y + xy^4] + c [x^2 y + xy^2],$ $t_\iota = c.$

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

$x \land \rho b = c x^4 + b^{-1} x^2 + c^{-1} x, x \land \sigma c = a x^4 + c^{-1} x^2 + a^{-1} x, x \land \alpha a = b x^4 + a^{-1} x^2 + b^{-1} x,$

$x \land \rho c = a^{-1} x^4 + a x^2 + c^{-1} x, x \land \sigma a = b^{-1} x^4 + b x^2 + a^{-1} x, x \land \alpha b = c^{-1} x^4 + cx^2 + b^{-1} x,$

$x^4 = x \land \rho b + x \land \sigma c + x \land \alpha a, x^2 = x \land \rho c + x \land \sigma a + x \land \rho b.$

Theorem 6. In $\mathbb{F}_8$, with $\land = \land_\alpha,$ the product is $x \times y = x^2 \land y^2 + x \land y^4 + x^4 \land y + x^4 \land y^2 + x^2 \land y^4,$ and so every function on $\mathbb{F}_8^6$ with values in $\mathbb{F}_8$ is a composition of constants, $\land, \land,$ and $(-)^2.$ Furthermore, we have $r(x) + s(x) + i(x) = x^2,$ and every function is a composition of constants, $\land, \land, r, s, i.$ As $x^2 = x \land_\rho c + x \land_\sigma a + x \land_\alpha b,$ every function is also a $\{k, \rho, \sigma, \iota\}$-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, $\land, \land,$ and $(-)^2,$ for $\land, \land$ a boolean structure on $\mathbb{F}_{2^n}$ associated to a normal basis, and $(-)^2$ the Frobenius map. There is a subset $V$ of $\text{GL}_n(\mathbb{F}_2)$ — of cardinal $4$ if $n$ is odd, and $3$ if $n$ is even — such that for every integer $k$, every function $\mathbb{F}_{2^n}^k \rightarrow \mathbb{F}_{2^n}$ 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 $b_i = (b_n)^i$. With some $\gamma_{i,j,k} \in \mathbb{F}_2$ (to be precised only for computing an explicit result, as we did for $n = 2, 3$), $\sum_{i,j,k} x_i b_j y_{k+i} = \sum_{i,j,k} \gamma_{i,j,k} x_i y_{k+i} b_j.$

We get for example $(x \land_\beta y^{2^{m^2}}) \land_\beta b_{i+1} = x_i y_{i-m} b_{i+1}.$ The general operator $x \mapsto y \land_\varphi z$, for an arbitrary basis $\varphi$ with matrix $A$ with respect to $\beta$ 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 $((A^{-1} z)^d)_{i,i} = (A^{-1} z)_{i,i}$) and is the general projector $x \mapsto P x$, 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 $\pi_i$ the matrix with 1 at $(i, i)$ and $(i + 1, i)$, for $i < n$, and $\pi_n$ the matrix with 1 at $(n, n)$ and $(1, n)$, we get $x^2 = x + (\sum_{i<n} \pi_i) + (\sum_{i=n} \pi_i) + (\sum_{i=n+1} \pi_i) + (\pi_n) & (n \text{ odd})$.

