An alternative way to classify some Generalized Elliptic Curves and their isotopic loops

M. Abou Hashish, L. Bénéteau

Abstract. The Generalized Elliptic Curves (GECs) are pairs (Q,T), where T is a family of triples (x,y,z) of "points" from the set Q characterized by equalities of the form $x.y=z$, where the law $x.y$ makes Q into a totally symmetric quasigroup. Isotopic loops arise by setting $x*y=u.(x.y)$. When $(x.y).(a.b)=(x.a).(y.b)$, identically (Q,T) is an entropic GEC and $(Q,*)$ is an abelian group. Similarly, a terentropic GEC may be characterized by $x^2.(a.b)=(x.a)(x.b)$ and $(Q,*)$ is then a Commutative Moufang Loop (CML). If in addition $x^2=x$, we have Hall GECs and $(Q,*)$ is an exponent 3 CML. Any finite terentropic GEC admits a direct decomposition in primary components and only the 3-component may eventually be non entropic, in which case its order is at least 81. It turns out that there are fifteen order 81 terentropic GECs (including just three non-entropic GECs). In class 2 CMLs the associator enjoys some pseudo-linearity: $(x*x',y,z)=(x,y,z)*(x',y,z)$. We are thus led to searching representatives in the set $\mathrm{AT}(n,m,K)$ of image-rank m alternate trilinear mappings from $(V(n,K))^3$ to $V(m,K)$ up to changes of basis in these K-vector spaces. Denote by $\alpha(n,m,K)$ the cardinal number of the sets of representatives. We establish that $\alpha(5,2,K)\leq 5$ whenever each field-element is quadratic; moreover $\alpha(5,2,\mathbb{F}_3)=6$ and $\alpha(6,2,\mathbb{F}_3)\geq 13$. We obtained a transfer theorem providing a one-to-one correspondence between the classes from $\mathrm{AT}(n,m,\mathbb{F}_3)$ and the rank $n+1$ class 2 Hall GECs of 3-order $n+m$. Now $\alpha(7,1,\mathrm{GF}(3^s))=11$ for any s. We derive a complete classification and explicit descriptions of the eleven Hall GECs whose rank and 3-order both equal 8. One of these has for automorphism group some extension of the Chevalley group $G_2(\mathbb{F}_3)$.

Keywords: totally symmetric quasigroups, terentropic quasigroups, commutative Moufang loops, generalized elliptic curves, extended triple systems, alternate trilinear mappings

Classification: 20N05, 14H52, 46G25

1. Introduction conventions and first examples

Let G be a non-empty set. An "unordered triple" from G, denoted by $((x,y,z))$ or simply $((xyz))$, is the equivalence class included in G^3 consisting of all the triples of the form (x',y',z') that one may derive from (x,y,z) by an arbitrary permutation of the three arguments.

By definition, a Generalized Elliptic Curve (GEC for short) is a pair (G,T), where T is a given family of unordered triples from the set G such that any pair (x,y) not necessarily distinct points of G is contained in exactly one triple

$((x, y, z))$ from T. Let us denote then $x.y = z$ and for any fixed element u from G we set $x \star_u y = u.(x.y)$. Both these binary laws are commutative. Besides, $u.(x.u) = x$, hence $(G, \star_u)$ is a commutative loop with identity element u; we call it the related loop of origin u. For any point x from G its "tangential" is the unique point t such that $((xxt))$ belongs to T. In case $t = x$ one says that x is an inflexion point. The set $I(G)$ of all the inflexion points is the set of the idempotent elements in the totally symmetric quasigroup $(G, .)$. The "rank" of a GEC (G, T) is the smallest cardinal number r such that G admits a generator subset whose cardinal is r. The entropic GECs are those in which $(x.y).(z.t) = (x.z).(y.t)$ identically. When this identity is only assumed to be fulfilled in any subsystem of rank ≤ 3, one says that (G, T) is a terentropic GEC (or TGEC). More particularly, the TGECs in which any point is an inflexion point are the Hall GECs (or HGECs for short).

Example 1.1. Let $P = \{a, b, c, d\}$ be a 4-element set. It may be provided in two ways with a GEC structure whose collection of triples is either
$T = \{((bcd)), ((bba)), ((cca)), ((dda)), ((aaa))\}$, or
$U = \{((bcd)), ((bba)), ((ccc)), ((dda)), ((aac))\}$. The ranks of (P, T) and (P, U) are 2 and 1 respectively. Any 4-order GEC need be isomorphic to either (P, T) or (P, U).

In fact, (P, T) is just a special case of "binary GEC": every elementary abelian 2 group $(B, +)$ may be classically endowed with a GEC structure whose triples $((x, y, z))$ are characterized by $x + y + z = 0$.

Example 1.2. Consider the direct product $Q = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ with typical element $X = (x, y, z)$. Q may be provided with a CML structure by the law $X * X' = (x+x', y+y', a+a'+3(x-x')(yz'-y'z))$. The set of triples (X, X', X'') characterized by $X'' = -(X * X')$ makes Q into a terentropic GEC. It is one of the three non entropic terentropic GECs of minimum order (81).

Example 1.3. Let $V = V(8, \mathbb{F}_3)$ be the 8-dimensional vector space over $\mathbb{F}_3$ with typical element $X = \sum_{1 \leq i \leq 8} x_i e_i$. For any two points X and Y let us set $X.Y = -X - Y + \delta(X, Y)e_8$ with:

$$\begin{aligned}\delta(X, Y) = (x_2y_3 - x_3y_2 + x_4y_7 - x_7y_4)(y_1 - x_1) + (x_5y_7 - x_7y_5)(y_2 - x_2) \\ + (x_6y_7 - x_7y_6)(y_3 - x_3) + (x_5y_6 - x_6y_5)(y_4 - x_4).\end{aligned}$$

This law makes V into a totally symmetric distributive quasigroup. The triples of the form $(X, Y, X.Y)$ provide V with a Hall GEC structure. It is a special example of the eleven 3^8-order Hall GECs of maximal rank 8.

It is quite obvious from the preceding examples that some trilinear skew-symmetric mappings are used to construct examples of terentropic GECs (see also [4], [8] and [14], [15], [18]). This aspect is to be developed in Section 4.

The GECs arose in combinatorics (where they are called "Extended Triple Systems") and in quasigroup theory (where one identifies them with the related totally symmetric quasigroups $(G, .)$). Before turning to structure theorems and classification results, let us recall a few geometrical facts so as to explain the terminology we employ (that comes mainly from Buekenhout [7], Keedwell [13] and Manin [17]). In the n-dimensional projective space $PG(n, K)$ over some field K consider $P = S_r(K)$, the set of regular (or non-singular) K-points of some absolutely irreducible cubic hypersurface S defined over K. The points x, y, and z from P are said to be collinear (notation $\mathrm{Col}(x, y, z)$) if there is a line L containing x, y and z and such that the intersection $L.S$ is either L or of the form $x + y + z$, each point turning up equally often as its intersection multiplicity (the addition notation we use there denotes only an intersection cycle; it has nothing to do with a binary operation). This three-place relation of collinearity $\mathrm{Col}(x, y, z)$ is clearly invariant under any permutation. Besides, for any pair x, y from P there exists at least one z such that $\mathrm{Col}(x, y, z)$. When $n > 2$, there are several such z in general. Nevertheless, z is uniquely determined when $n = 2$ and one may then state the well-known following result:

Theorem 1.1 (Lamé [17]). *If S is a curve then the collection of the triples $((x, y, z))$ of collinear points makes P into an entropic* GEC *and, for any u from S, the loop of origin u $(P, *_u)$ is an abelian group.*

Theorem 1.2 (Buekenhout's classification [7]). *There are up to isomorphism exactly twenty six* GECs *of order* ≤ 8. *Only thirteen ones are entropic; and they are all related to projective elliptic curves except the order* 8 *binary one.*

Remark 1.1. Clearly, elementary abelian groups of order p^t with $t > 2$ may not occur as groups $(P, *)$ arising from finite projective cubic curves $S \subset PG(2, \mathbb{F}_q)$ that are generated by at most 2 elements: one knows that these groups $(P, *)$ are direct products of at most two cyclic groups of the form: $\mathbb{Z}_n \times \mathbb{Z}_d$, where n and d are non negative integers such that d divides both n and $q-1$. Their orders satisfy $q + 1 - 2\sqrt{q} \leq |P| \leq q + 1 + 2\sqrt{q}$ (Hasse's theorem see [16]). The actual value of $|P|$ may be computed by several algorithms (see for instance Schoof [21]). They are used for implementing secure public-key cryptosystems, because they contain large cyclic groups in which the "logarithm problem" (namely the determination of an integer l such that $la = b$) is presently considered as intractable (see [16] and [11]).

For the remainder of this section we restrict ourselves to the case $n > 2$. Thus S is an hypersurface of dimension > 1. Assume moreover that S admits a non-singular point x such that the intersection "hypercurve" $C_x = T_x \cap S$ of the tangent hyperplane T_x with S is geometrically irreducible, reduced and that x is not conical in C_x. Then consider a quotient $Q = P/R$ of $P = S_r(K)$ with respect to an "admissible relation" R, namely a compatible equivalence relation in P such that the natural way to factorize the collinearity yields a ternary relation

$\mathrm{Col}_R(X, Y, Z)$ such that for any X and Y from Q there is just one class Z such that $\mathrm{Col}(x, y, z)$ holds for 3 suitable representatives. Then:

Theorem 1.3 (Manin and Bel'skii [17]). *In the factor set $Q = P/R$, the collection T of the triples of classes X, Y, Z such that $\mathrm{Col}_R(X, Y, Z)$ holds provides Q with a structure of* TGEC *in which any tangential is an inflexion point* (*if* (XXZ) *belongs to T so does* (ZZZ)). *Its inflexion point subset $I(Q)$ is a subsystem, and it is a* HGEC. *Moreover, there is some binary subsystem B such that (Q, T) splits as a direct product of $I(Q)$ by B.*

The difficult problem of constructing eventually an hypersurface S in which $I(Q)$ is not entropic seems to be still unsolved (see [17], [8] and [3]).

2. The kinship between Terentropic Generalized Elliptic Curves and CMLs

Our aim is to classify some TGECs up to isomorphism. Any TGEC has an essentially unique related CML $(G, *_u)$. But the knowledge of the related loop $(G, *_u)$ only determines (G, T) up to isotopy. Let us be more precise.

First, let us deal briefly with the classical correspondence between entropic GECs and abelian groups. One may easily check that, if (Q, T) is a GEC and u an arbitrary element from Q, then (Q, T) is entropic if and only if the related loop $(Q, *_u)$ is an abelian group whose structure does not depend on the choice of the "origin" u. Conversely, if $(A, +)$ is an abelian group then for any c from A the unordered triples $((xyz))$ defined by the condition $x + y + z = c$ endow the underlying set A with an entropic GEC structure. Any entropic $\mathrm{GEC}(G, T)$ may be constructed in this way from an abelian group that is unique up to isomorphism. These assertions are to be subsumed by the two following properties that establish that the TGECs are similarly related to the CMLs (namely to the loops $(G, *)$ such that $(x * x) * (y * z) = (x * y) * (x * z)$ identically).

Proposition 2.1. *Let (G, T) be a* GEC *with symmetric law $x.y$. Let us set $x^2 = x.x$. Consider an arbitrary fixed element u from G. When (G, T) satisfies one of the following four conditions then it satisfies all of them:* (i) (G, T) *is terentropic;* (ii) $x^2.yz = xy.xz$ *identically;* (iii) $x.yz = x^2y.xz$ *identically;* (iv) $(G, *_u)$ *is a* CML. *Moreover, in this case the loop $(G, *_u)$ does not depend on the choice of u up to isomorphism. It admits u^2 as an associatively central element. The triples $((xyz))$ from T may be characterized by $x *_u y *_u z = u^2$.*

Proposition 2.2. *Let $(G, +)$ be a* CML *with identity element e and c an arbitrary central element from G. Then the underlying set G organized with the family of unordered triples of the form $((x, y, c - x - y))$ is a* TGEC. *Any* TGEC *may be obtained in this way. Besides, from the* $\mathrm{GEC}(G, T_c)$ *one may recover the initial* CML *by taking the related loop of origin e.*

Recall that the "center" $Z = Z(G)$ of a CML $(G, +)$ is as usual defined as the set of the elements c whose behaviour is associative with respect to any pair x, y of elements from G (namely, $(x + y) + c = x + (y + c)$). A well-known property of the abelian group Z is that it contains the set $\theta(G) = \{3t \mid t \in G\}$ as a subgroup (see for instance [8]). We need a sufficient condition for two elements c and d from Z to give rise to isomorphic GECs.

Proposition 2.3. *Under the hypothesis of the previous proposition, if $c \in Z(G)$ then for any $\epsilon = \pm 1$ and for any t from $Z(G)$ the sum $d = \epsilon c + 3t$ belongs to $Z(G)$ and the corresponding* TGECs *(G, T_c) and (G, T_d) are isomorphic.*

Proof: The mapping $f(x) = x' = \epsilon x + t$ is clearly a permutation of G and $f^{-1}(x') = \epsilon x' - t$. Besides, $x + y + z = c$ implies $(\epsilon x + t) + (\epsilon y + t) + (\epsilon z + t) = \epsilon c + 3t$, since t is central. Thus $x' + y' + z' = d$. Conversely, this relation implies that $x + y + z = c$. This proves that $f(T_c) \subset T_d$ and $f^{-1}(T_d) \subset T_c$ as required. □

The foregoing property has some obvious consequences that prove to be very useful.

Corollary 2.4. *The* TGECs *admitting an inflexion point may be described from their isotopic* CML *by a family of triples characterized by $x + y + z = 3t$, where t is any element from G.*

Proof: One may say then that (G, T_{3t}) is isomorphic to (G, T_e), where e is the identity element. □

Corollary 2.5. *A* CML *$(G, +)$ admits up to isomorphism exactly one isotopic* TGEC *if and only if $\theta(G) = Z(G)$.*

Proof: Otherwise for $c \in Z$ and $c \notin \theta$ the TGEC (G, T_c) has no inflexion point and may not be isomorphic to (G, T_e). □

Corollary 2.6. *Any finite* CML *whose order is prime to* 3 *is an abelian group and has only one related* TGEC.

Proof: Since $\omega = |G|$ satisfies $3h + \omega k = 1$, any x from G obeys $3hx = x$, so that $\theta(G) = G$. □

Any finite CML $(G, +)$ admits a canonical decomposition as a direct product $H \times A$, where H is a (possibly non associative) 3-power order CML and A is an abelian group whose order is prime to 3. In view of the previous property one knows that A admits just one isotopic GEC. One needs just to classify the elements c from $Z(H)$ that give rise to non isomorphic TGEC (H, T_c) so as to list all the TGECs related to $(G, +)$. Unfortunately, this classification is not easy in general.

In the special case of abelian group, Schwenk [24] provided simple representatives of the TGECs (G, T_c) up to isomorphism. He showed that if the unique decomposition of the 3-component H of G as a direct product of 3-power order cyclic groups involves exactly k non isomorphic cyclic factors then there are exactly $k+1$ non isomorphic such TGECs. Let us be more precise:

Theorem 2.7 (Schwenk [24]). *Let an abelian group $(G,+)$ be written as a direct product $H \times A$, where A has an order prime to 3 and H is a 3^s-order group isomorphic to $(\mathbb{Z}_{3^{r_1}})^{l_1} \times (\mathbb{Z}_{3^{r_2}})^{l_2} \times \cdots \times (\mathbb{Z}_{3^{r_k}})^{l_k}$ with $l_1r_1 + l_2r_2 + \cdots + l_kr_k = s$ and $r_1 < \cdots < r_k$. Then there are exactly $k+1$ pairwise non isomorphic* TGECs *of the form (G, T_c): one with $c = e$ and k* TGECs *without inflexion point whose family of triples $T_{c_1}, T_{c_2}, \ldots, T_{c_k}$ arise by taking c_i as an arbitrary generator of an arbitrary 3^{r_i}-order cyclic factor subgroup in the decomposition of H.*

Proof: If H is a n-order cyclic group spanned by c then each d from H is related modulo $3H$ either to $\mp c$ or to the identity element e, so that (H, T_d) is isomorphic to either (H, T_c) or (H, T_e). We have already seen that when n is prime to 3 then (H, T_d) is isomorphic to (H, T_e). Schwenk proved that if $r \le t$ then the two GECs $(\mathbb{Z}_{3^r} \times \mathbb{Z}_{3^t}, T_{(0,1)})$ and $(\mathbb{Z}_{3^r} \times \mathbb{Z}_{3^t}, T_{(1,1)})$ are isomorphic by the mapping

$$(a,b) \mapsto \quad ((a+b) \text{ modulo } 3^r, b).$$

As a consequence, one may prove that if H is a 3-power order abelian group admitting a decomposition as a direct sum of subgroups $\langle c_{i,j} \rangle$ for $j = 1, 2, \ldots, k$ and $i = 1, 2, \ldots, l_j$, whose orders are $O(c_{i,j}) = 3^{r_j}$ with $r_1 < \cdots < r_k$, then any GEC without inflexion point related to H is isomorphic to some (H, T_c), where $c \in \{c_{1,1}, c_{1,2}, \ldots, c_{1,k}\}$. Furthermore, Schwenk checked that in $(H, T_{c_{i,j}})$ the permutation:

$$x \mapsto x^2 = c - 2x$$

is decomposable in disjoint cycles of minimum length 3^{r_j} which establishes that the k possible choices lead to pairwise non isomorphic GECs as required (for more details see [24]). □

As a consequence of the foregoing statements and taking into account [3], one may state the:

Theorem 2.8. *Any finite* TGEC *that is not entropic has an order which is a multiple of* 81. *There are exactly fifteen order* 81 TGECs *including twelve entropic* GECs *and just three that are not entropic. If $\mathbb{L}_3$ and $\mathbb{N}_3$ are the non associative order* 81 CMLs *with respective exponent* 3 *and* 9 *and identity element u and v and if c is a central element of $\mathbb{L}_3$ distinct from u then the correspondence between the* TGECs *and the related groups or loops is as follows:*

Groups and CMLs *of order* 81	*Number and explicit descriptions related* GECs (G, T_c)
$(\mathbb{Z}_3^4, +)$	$2 : (\mathbb{Z}_3^4, T_{(0,0,0,0)})$ *and* $(\mathbb{Z}_3^4, T_{(0,0,0,1)})$
$(\mathbb{Z}_3^2 \times \mathbb{Z}_9, +)$	$3 : (\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(0,0,0)}), (\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(1,0,0)})$ *and* $(\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(0,0,1)})$
$(\mathbb{Z}_9^2, +)$	$2 : (\mathbb{Z}_9^2, T_{(0,0)})$ *and* $(\mathbb{Z}_9^2, T_{(0,1)})$
$(\mathbb{Z}_3 \times \mathbb{Z}_{27}, +)$	$3 : (\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(0,0)}), (\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(1,0)})$ *and* $(\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(0,1)})$
$(\mathbb{Z}_{81}, +)$	$2 : (\mathbb{Z}_{81}, T_0)$ *and* $(\mathbb{Z}_{81}, T_1)$
$(\mathbb{L}_3, \star)$	$2 : (\mathbb{L}_3, T_u)$ *and* $(\mathbb{L}_3, T_c)$
$(\mathbb{N}_3, \star)$	$1 : (\mathbb{N}_3, T_v)$

Table 1*: The fifteen order* 81 TGECs

PROOF: One knows already from [6] that any finite CML $(G, +)$ has an order n such that 3^4 divides n. If $n = 81$, then $G \simeq \mathbb{L}_3$ or $G \simeq \mathbb{N}_3$. Since $\theta(\mathbb{N}_3) = Z(\mathbb{N}_3)$, there is just one GEC related to $(\mathbb{N}_3)$. The rest follows easily from the foregoing properties. $\square$

3. The classification of alternate trilinear mappings

Let us turn now to the determination of the orbits of the alternate trilinear mappings from V^3 to W under the natural action of the linear groups $\mathrm{GL}(V)$ and $\mathrm{GL}(W)$ of the K-vector spaces V and W. We deal with the general problem so as to state the classification results at their natural level of generality. Afterwards we focus on the special case $K = \mathbb{F}_3$ in view of by-products concerning the Hall GECs.

First a few conventions. Let K be a commutative field. Denote by $V(n, K)$ the n-dimensional K-vector space. If $V = V(n, K)$ and $W = V(m, K)$, we designate as $\mathrm{AT}(n, m, K)$ the set of all the alternate (or symplectic, skew-symmetric) trilinear mappings t from V^3 to W whose image has rank m. Any pair of linear mappings g and h from $\mathrm{GL}(V)$ and $\mathrm{GL}(W)$ has a natural action on the elements t from $\mathrm{AT}(n, m, K)$, since the mapping $t'(x, y, z) = ht(g(x), g(y), g(z))$ also belongs to $\mathrm{AT}(n, m, K)$. One says then that t' and t are "projectively equivalent" and in case $h = \mathrm{id}$, that t' and t are "equivalent". We want to classify $\mathrm{AT}(n, m, K)$ in orbits under the action of $\mathrm{GL}(V) \times \mathrm{GL}(W)$, or under the action of $\mathrm{GL}(V)$. Let $\underline{\alpha}(n, m, K)$ and $\alpha(n, m, K)$ be the cardinal numbers of any set of representatives. The "classes" are the orbits under the action of $\mathrm{GL}(V)$, their cardinal number is $\alpha(n, m, K)$.

Let t be a given element $\mathrm{AT}(n, m, K)$, where $t : V^3 \to W$. For any subspace U of V we define its "orthogonal" $U^\perp$ as the subset of the elements x from V satisfying $t(x, y, z) = 0$ for any y and z from U. When $U^\perp \cap U \neq \{0\}$ (resp. $U^\perp \supset U$), we say that U is "singular" (resp. "totally isotropic"). In case $V^\perp \neq \{0\}$, the trilinear mapping itself is said to be singular. Designate as $\tau(n, m, K)$ and $\underline{\tau}(n, m, K)$ the cardinal numbers of the family of the orbits of non singular mappings from

$\mathrm{AT}(n,m,K)$ under the action of $\mathrm{GL}(V)$ and $\mathrm{GL}(V)\times\mathrm{GL}(W)$, respectively. The "rank" $rg(t)$ is the codimension of $V^{\perp}$ in the departure space $V=V(n,K)$ (we call it sometimes the "departure-rank" when some confusion with the rank of $t(V^3)$ is to be avoided). Thus t is singular if and only if $rg(t)<n$. Observe that the following obvious equality holds: $\alpha(n,\binom{n}{3},K)=1=\tau(n,\binom{n}{3},K)$. One may also check that:

Proposition 3.1 (Cases of vanishing)**.** *Let K be any field. If $n<2$ or if $m>\binom{n}{3}$ then $\alpha(n,m,K)=0=\tau(n,m,K)$. But for $n\geq 3$, whenever $m\leq\binom{n}{3}$ then both cardinal numbers $\alpha(n,m,K)$ and $\tau(n,m,K)$ differ from 0, except for: $\tau(4,1,K)=0$.*

Theorem 3.2 (Starting values)**.** *For any field K, we have the following additive formula: $\alpha(n,m,K)=\alpha(n-1,m,K)+\tau(n,m,K)$. Furthermore, $\alpha(4,1,K)=1=\alpha(4,m,K)=\tau(4,m,K)$ for $m=2,3,4$; besides, $\tau(5,1,K)=1$, so that $\alpha(5,1,K)=2$.*

Let us sum up what we know about the classification if $m=1$. The elements from $\mathrm{AT}(n,1,K)$ are just the non-vanishing trilinear alternate forms. Their classification reduces to determining the orbits of 1-linear forms of the exterior product Λ^3V, and by duality this is equivalent to classifying non-vanishing "trivectors" from Λ^3V in orbits under the natural action of $\mathrm{GL}(V)$.

Theorem 3.3 (Gurevitch [12])**.** *If K is algebraically closed then $\alpha(n,1,K)$ and $\tau(n,1,K)$ are finite if and only if $n\leq 8$.*

Property 3.4 (Sum formula)**.** *If $n\geq 6$ then $\alpha(n,1,K)=2+\sum_{6\leq d\leq n}\tau(d,1,K)$, where $\tau(d,1,K)$ are non vanishing cardinal numbers depending on the field K.*

The next two partial classifications have been proved in [20].

Proposition 3.5. *The trilinear alternate forms of departure V^3, where $V=V(n,K)$ admits a totally isotropic hyperplane, make up $k=\left\lfloor\frac{(n-1)}{2}\right\rfloor$ classes, where k is the largest integer such that $2k<n$. If n is even then all these forms are singular, while if n is odd then one and only one of the k classes consists of non singular forms.*

Proposition 3.6. *In $\mathrm{AT}(6,1,K)$, the forms admitting a singular hyperplane make up exactly four classes. If K is quadratically closed, these four classes cover entirely $\mathrm{AT}(6,1,K)$, so that $\alpha(6,1,K)=4$.*

Theorem 3.7 (Number of non equivalent forms)**.** *Let K be an algebraically closed field and $\mathbb{F}_q=\mathrm{GF}(q)$ the q-element finite field. The maximum number of pairwise non equivalent forms of departure V^3, where $V=V(n,K)$ or $V(n,\mathbb{F}_q)$, are given by the following table:*

dimension n	$n \leq 2$	3	4	5	6	7	8	≥ 9
$\tau(n,1,K)$	0	1	0	1	2	5	?	∞
$\alpha(n,1,K)$	0	1	1	2	4	9	?	∞
$\tau(n,1,F_q)$	0	1	0	1	3	$5+\gcd(q-1,3)$	?	?
$\alpha(n,1,F_q)$	0	1	1	2	5	$10+\gcd(q-1,3)$	?	?

Table 2: Number of forms when the field is either algebraically closed or finite

PROOF: The fact that $\tau(7,1,K)=5$ and that therefore $\alpha(7,1,K)=\tau(7,1,K)+4=9$ is due to Schouten (see [23]). The values of $\alpha(n,1,\mathbb{F}_q)$ for $n \leq 7$ may be derived from Cohen and Helminck [9] that concerns the more general case where the base field is perfect and of cohomogical dimension at most 1. One may also refer to Revoy [21] and Noui [19]. These works provide among other results the numbers of projectively non equivalent forms starting from any finite 7-dimensional vector space: $\underline{\tau}(7,1,\mathbb{F}_3)=6$ and $\underline{\alpha}(7,1,\mathbb{F}_3)=11$.

For the dimension 8 or ≥ 9, the cells with a question mark "?" contain finite numbers that are still unknown without some additional specification for the field. $\square$

Remark 3.1. More special classifications were obtained by Vinberg [26] for $\mathrm{AT}(9,1,\mathbb{C})$ and by Djokovic (cf. [10]) for $\mathrm{AT}(8,1,\mathbb{R})$, where $\mathbb{C}$ and $\mathbb{R}$ are respectively the field of complex numbers and the field of real numbers. Besides, for K algebraically closed of characteristic 0 one knows that $\alpha(8,1,K)=22$ and $\tau(8,1,K)=13$ (see Gurevitch [12]).

Let us turn now to an explicit description of some "simple" sets of representatives with respect to a canonical basis $e_i, i=1,2,\ldots,n$, of $V=V(n,K)$.

The vectors from V are considered as column-vectors with coefficients from K. The 1-form from the dual V^* are identified with line-vectors $u^\intercal$ with coefficients from K. Any alternate trilinear form t from V^3 to K gives rise to an element t^* of the dual $(\Lambda^3 V)^*$ that is classically isomorphic to $\Lambda^3 V^*$. Any trivector $u_1^\intercal \Lambda u_2^\intercal \Lambda u_3^\intercal$ of $\Lambda^3 V^*$ is thereby identified with the alternate trilinear mapping defined as follows:

$$u_1^\intercal \Lambda u_2^\intercal \Lambda u_3^\intercal(x_1,x_2,x_3)=\sum_{\sigma\in S_3}\mathrm{sign}(\sigma)\prod_{i=1}^3 u_i^\intercal(x_{\sigma(i)}).$$

So the $e^*_{ijk}=e_i^\intercal \Lambda e_j^\intercal \Lambda e_k^\intercal$, where $1\leq i<j<k\leq n$, make up a basis of $\Lambda^3 V^*$.

For any K in $\mathrm{AT}(6,1,K)$, any form of rank ≤ 5 is equivalent to $f_1=e^*_{123}$ or to $f_2=e^*_{123}+e^*_{145}$ whose ranks are 3 and 5, respectively. Any rank 6 form admitting a 5-dimensional singular subspace is equivalent to one and only one of the two following forms: $f_3=e^*_{123}+e^*_{456}$ or $f_4=e^*_{162}+e^*_{243}+e^*_{135}$.

If K is quadratically closed then any t form $\mathrm{AT}(6,1,K)$ is equivalent to one and only one of the previously defined forms f_1, f_2, f_3 and f_4.

Convention: Assume now that K is a characteristic k commutative field and that λ is a scalar from K such that:

(i) either $k > 2$ and λ is not a square in K;

(ii) or $k = 2$ et $x^2 + \lambda x + 1$ is an irreducible polynomial in $K[x]$.

Let us set:

$g_\lambda = e^*_{123} + \lambda(e^*_{156} + e^*_{345} + e^*_{426})$ if $k \neq 2$,

$g_\lambda = e^*_{126} + e^*_{153} + e^*_{234} + \lambda(e^*_{156} + e^*_{345} + e^*_{426}) + (\lambda^2 + 1)e^*_{456}$ if $k = 2$.

In $\mathrm{AT}(7, 1, K)$ there are always at least 5 pairwise non equivalent rank 7 alternate trilinear forms, namely: $f_5 = e^*_{123}+e^*_{456}+e^*_{147}$; $f_6 = e^*_{152}+e^*_{147}+e^*_{163}+e^*_{243}$; $f_7 = e^*_{146} + e^*_{157} + e^*_{245} + e^*_{367}$; $f_8 = e^*_{123} + e^*_{145} + e^*_{167}$;
$f_9 = e^*_{123} + e^*_{456} + e^*_{147} + e^*_{257} + e^*_{367}$.

When K is algebraically closed, Schouten [23] established that any t from $\mathrm{AT}(7, 1, K)$ is equivalent to one of the 9 forms $f_i, i = 1, 2, \ldots, 9$.

Theorem 3.8 (Cohen and Helminck [9])**.** *Let K be a perfect field such that the Galois group of its algebraic closure has cohomogical dimension at most* 1*. Then any form t from $\mathrm{AT}(7, 1, K)$ that is not equivalent to one of the f_i for $i = 1, 2, \ldots 9$, has rank $r = 6$ or 7, and:*

(i) *if $r = 6$ and t is equivalent to one of the foregoing defined g_λ;*

(ii) *if $r = 7$ then t is equivalent to either one of the forms: $e^*_{147} + g_\lambda$, or to a form of type μf_9, where μ is an element of K that is not cubic in K.*

In the case of a finite field $\mathbb{F}_q$, the preceding theorem applies, since $\mathbb{F}_q$ is then a perfect field of cohomogical dimension ≤ 1. One may say that $\tau(7, 1, \mathbb{F}_q) = 6$ and $\alpha(7, 1, \mathbb{F}_q) = 11$, whenever $q - 1$ is prime to 3; otherwise $\tau(7, 1, \mathbb{F}_q) = 8$ and $\alpha(7, 1, \mathbb{F}_q) = 13$ (see [9] and also [19]). Both cases occur if $q = 2^m$; more precisely, either m is odd and $\tau(7, 1, \mathrm{GF}(2^m)) = 6$, or m is even and $\tau(7, 1, \mathrm{GF}(2^m)) = 8$. On the opposite, in the characteristic 3 case we always have $\tau(7, 1, \mathrm{GF}(3^s)) = 6$ and $\alpha(7, 1, \mathrm{GF}(3^s)) = 11$.

Corollary 3.9. *Any form t from $\mathrm{AT}(7, 1, \mathrm{GF}(3^s))$ can be conveniently represented by:*

(i) *either by f_1, f_2, f_3, f_4 and $g_{(-1)}$ when t has rank at most 6;*

(ii) *or by f_5, f_6, f_7, f_8, f_9 and $(e^*_{147} + g_{(-1)})$ when t is non singular.*

In the remainder of this section, we investigate the classification of alternate trilinear mappings whose image-rank m is at least 2. As far as we know, there has never been any systematic attempt to classify $\mathrm{AT}(n, m, K)$ for $m > 1$ apart from the very first step $n = 4$. We shall assume that some basis $B = \{e_i; i = 1, 2, \ldots, n\}$ is chosen in the departure space $V = V(n, K)$. Designate by e_{ijk} the image $t(e_i, e_j, e_k)$ in $W = V(m, K)$. Our first task is to make a suitable choice of B so as to maximize the total number of zero-image triples (e_i, e_j, e_k).

Theorem 3.10 (Simplified basis)**.** *Suppose there exists a t in* $\mathrm{AT}(n,m,K)$ *whose image-rank m is at least 2. Then $n \geq 4$ and V contains a 4-rank system $S = \{e_1, e_2, e_3, e_4\}$ such that:*

(a) *e_{123} and e_{234} are independent,*
(b) *$e_{124} = 0 = e_{134}$.*

If, furthermore, $m = 2$ then one may complete S in a basis obeying the following properties:

(c) *$e_{23i} = 0 = e_{12l} = e_{13h}$ holds for any $i \geq 5$, $l \geq 6$ and $h \geq 7$ with $i, j, k \leq n$;*
(d) *there exists β and γ from $\{0,1\}$ with the following equalities: $e_{125} = \beta e_{234} = e_{136}$ and $e_{135} = \gamma e_{234}$.*

Proof: See [1]. □

Any t in $\mathrm{AT}(n,2,K)$ may be conveniently represented by defining relations of the form $(e_{ijk}; e_{pqr})$ or $(e_{ijk} = e_{uvw}; e_{pqr})$ in which we mean that:

(i) the images e_{ijk} and e_{pqr} are non collinear;
(ii) $e_{xyz} = 0$ for any triple of subscripts x, y, z such that $x < y < z$ that do not appear in the defining relation;
(iii) eventually some explicitly stated equalities are obeyed (as $e_{ijk} = e_{uvw}$ in the second defining set).

Theorem 3.11. *If K is a field in which any element is a square then there are at most five pairwise non equivalent alternate trilinear forms in* $\mathrm{AT}(5,2,K)$*, namely*

$t_1 = (e_{125}; e_{234})$,
$t_2 = (e_{123} = e_{145}; e_{234})$,
$t_3 = (e_{123} = e_{245}; e_{234})$,
$t_4 = (e_{123}; e_{145})$,
$t_5 = (e_{123} = e_{245}; e_{145} = e_{234})$.

Proof: See [1]. □

Theorem 3.12 (Razafimanantsoa [20])**.** $\mathrm{AT}(5,2,\mathbb{F}_3)$ *splits into 6 classes whose representatives are t_1, t_2, t_3, t_4, t_5 and $t_6 = (e_{123} = e_{245}; e_{234} = e_{125})$. Moreover,* $\mathrm{AT}(5,3,\mathbb{F}_3)$ *contains at least 17 classes.*

We established by a computational approach that:

Theorem 3.13. *There are at least 7 pairwise non equivalent non singular forms in* $\mathrm{AT}(6,2,\mathbb{F}_3)$*, namely:*

$t_7 = (e^*_{123} = e^*_{346} = e^*_{145}; e^*_{234})$,
$t_8 = (e^*_{123} = e^*_{245} = e^*_{346}; e^*_{234} = e^*_{145})$,
$t_9 = (e^*_{123} = e^*_{145}; e^*_{234} = e^*_{456})$,
$t_{10} = (e^*_{123}; e^*_{145} = e^*_{456})$,
$t_{11} = (e^*_{123} = e^*_{245} = e^*_{346}; e^*_{234} = e^*_{125} = e^*_{456})$,

$t_{12} = (e^*_{123} = e^*_{346}; e^*_{145})$,
$t_{13} = (e^*_{123}; e^*_{145}$ *and* $e^*_{345} = e^*_{123} + e^*_{234})$.
Hence $\alpha(6, 2, \mathbb{F}_3) \geq 7 + 6 = 13$.

Proof: We already know that the singular mappings t from $\mathrm{AT}(6, 2, \mathbb{F}_3)$ make up 6 distinct classes whose representatives are the previously defined t_1, t_2, t_3, t_4, t_5 and t_6. It remained to check that the seven remaining ones were pairwise non equivalent and non singular. We computed for each $t = t_i$ the number $n_k(t)$ of hyperplanes H such that restriction of t to H has an image-rank equal to k where $k = 0, 1, 2$. It turns out that $n_1(t_i) \neq n_1(t_j)$ for every two $i \neq j$, except for t_6 and t_{11} that we may distinguish by remarking that $n_0(t_6) = 1 \neq 0 = n_0(t_{11})$. So the couple of invariants (n_0, n_1) shows that any two distinct t_i and t_j are not equivalent which validates our lower bound 13 for $\alpha(6, 2, \mathbb{F}_3)$, since $\alpha(6, 2, \mathbb{F}_3) = \tau(6, 2, \mathbb{F}_3) + \alpha(5, 2, \mathbb{F}_3) \geq 7 + 6$. For more details see [1]. □

Let us turn now to combinational by-products for Hall GECs and exponent 3 CMLs. Concerning the classification of exponent 3 CMLs of small orders, one knows already that there are exactly 12 such loops of order $\leq 3^6$ and also 13 such loops of order 3^7. Among the 3^8-order ones that differ from the elementary abelian 3-group, we know that their rank r obeys $4 \leq r \leq 7$, and that $r = 4$ corresponds to exactly four such loops. As a consequence of $\alpha(7, 1, \mathbb{F}_3) = 11$, we are presently able to establish the:

Theorem 3.14. *There are up to isomorphism exactly* 11 *rank* 7 *exponent* 3 CMLs *of order* 81*, and their related* GECs *make up* 22 *isomoprhy classes, including* 11 GECs *without inflexion point and* 11 *Hall* GECs.

This new result is less important for future investigations than the process we use to translate classification problems concerning class 2 exponent 3 finite CMLs into a search of representatives in some suitable $\mathrm{AT}(n, m, \mathbb{F}_3)$.

Let (E, T) be a HGEC of order 3^{n+m} and of rank $n + 1$. Designate by: $u, e_1, e_2, \ldots, e_n$ a generator subset of E and by $(E, +)$ the exponent 3 CML related to the origin u. We may endow E with an external law $(\lambda, x) \longmapsto \lambda x$ whose domain of operators λ is $\mathbb{F}_3$. Now Moufang loops are classically di-associative, thus any subloop generated by two elements is isomorphic to some vector space $V(s, \mathbb{F}_3)$ with s$\leq$ 2. Assume that (E, T) is not entropic, which means that $(E, +)$ is not associative, so that the associator: $\Delta(x, y, z) = ((x+y)+z) - (x+(y+z))$ does not vanish identically. Designate as $D(E)$ the "derived subloop", namely the subloop spanned by all the associators. The abelian quotient $A = q(E) = E/D(E)$ may be viewed as a $\mathbb{F}_3$-space isomorphic to $V(n, \mathbb{F}_3)$. If one denotes by $\overline{x}$ the coset of any element x modulo $D(E)$ then a basis of A is provided by $\overline{e}_i, i = 1, 2, \ldots, n$.

By convention, in case any associator is central (namely when $D(E) \subset Z(E)$), (E, T) and $(E, +)$ are said to be centrally nilpotent of class 2 (we shall say "of class 2" for short). For more details about the nilpotent properties for CMLs we refer the reader to [8], [6] and [2].

Theorem 3.15 (Associator-factorization). *If (E,T) is of class 2, of rank n and 3-order $n+m$, then:*

(i) *$D(E)$ is a m-dimensional $\mathbb{F}_3$-vector space admitting as a generator set the collection of the $\binom{n}{3}$ associators: $\Delta(e_i,e_j,e_k)$ for $1 \le i < j < k \le n$;*

(ii) *there exists a unique alternate trilinear mapping δ from A^3 to $D(E)$, so that $\delta(\overline{x},\overline{y},\overline{z}) = A(x,y,z)$ holds for any x, y and z from E; and $\delta \in \mathrm{AT}(n,m,\mathbb{F}_3)$;*

(iii) *the unique linear mapping $\overline{\delta}$ from $\Lambda^3 A$ onto $D(E)$ satisfying $\delta(\overline{x}\Lambda\overline{y}\Lambda\overline{z}) = A(x,y,z)$ has a kernel R that determines completely (E,T) and $(E,+)$ up to isomorphism.*

Proof: See [1] for details. The mapping δ has an image of rank m, and $\overline{\delta}$ is clearly surjective onto $D(E) \simeq V(m,\mathbb{F}_3)$. Its kernel $R = \mathrm{Ker}(\overline{\delta})$ may be naturally identified with the set of defining relations of the loop $(E,+)$, which completes the justification. □

By definition, δ is then said to be the "factorized associator" of (E,T) and $(E,+)$.

Let us now reverse the process, from a given alternate trilinear mapping from $\mathrm{AT}(n,m,\mathbb{F}_3)$ we want to recover corresponding HGECs and exponent 3 CMLs of class 2.

Consider an arbitrary codimension m subspace R in $\Lambda^3 V$, where $V = V(n,\mathbb{F}_3)$, vector space with a fixed basis e_i, $i = 1,2,\dots,n$. The quotient $W = \Lambda^3 V/R$ is trivially generated by the $\binom{n}{3}$ cosets of the trivectors: $e_{ijk} = (e_i\Lambda e_j\Lambda e_k + R)$ where $1 \le i < j < k \le n$.

Every vector x from the direct sum $E = V \oplus W$ may be written as a linear combination, say

$$x = \sum_{i=1,2,..,n} x_i e_i + \sum_{1\le i<j<k\le n} x_{ijk}\overline{e_{ijk}},$$

where x_i and x_{ijk} belong to $\mathbb{F}_3$.

One may define an exponent 3 CML binary law by setting

$$x * y = x + y + \sum_{1\le i<j<k\le n} (x_i y_j - y_i x_j)(x_k - y_k)\overline{e_{ijk}},$$

The so-determined sum $x*y$ is well-defined, though the x_{ijk}'s are not uniquely determined from x. A straightforward verification proves that $(E,*)$ has class 2. The family of unordered triples $((x,y,z))$ characterized by $x*y*z = 0$ endows the set E with a structure of HGEC of class 2 whose factorized associator is

$$\delta(\overline{x},,\overline{z}) = \Delta(x,y,z) = \sum_{1\le i<j<k\le n} e^*_{ijk}(x,y,z)\overline{e_{ijk}}.$$

Proposition 3.16. *Among the rank $n+1$ HGECs of 3-order $n+m$, the foregoing process allows the explicit construction of:*

(i) *all those obeying $m = 1, 2$ or 3;*
(ii) *the class 2 ones satisfying $4 \leq m \leq \binom{n}{3}$.*

PROOF: The basic fact is that rank n exponent 3 CML of order 3^{n+m} can reach a nilpotency class > 2 only in case $m \geq 4$ (see [6], [2]). Now it is quite clear from the preceding theorem that we may obtain any class 2 exponent 3 CML. As a matter of fact, the free object $L_{n,2}$ spanned by n elements in the variety of exponent 3 CML is known as a loop whose order is $3^{n+\binom{n}{3}}$, and our process of construction describes explicitly any factor-loop $L_{n,2}/R$ where R is an arbitrary (normal) subloop contained in $D(L_{n,2}) = Z(L_{n,2})$, which is a $\binom{n}{3}$-order elementary 3-group.

□

In our explicit-recovering process we established in particular that any non-vanishing alternate $\mathbb{F}_3-$ trilinear mapping δ arises as a factorized associator of an exponent 3 CML of class 2. Moreover, δ is singular if and only if $(E, *)$ is decomposable as a direct product $F \times C$ of a non trivial central factor ($\{0\} \neq C \subset Z(E, *)$) by a smaller loop. One says then that $(E, *)$ and its related HGEC are "centrally reducible".

Theorem 3.17 (Number of isomorphy classes)**.** *For any $n \geq 3$ and $m \geq 1$, the integer $\alpha(n, m, \mathbb{F}_3)$ coincides with the maximum number of pairwise non isomorphic rank $(n+1)$ HGECs of $3-$ order $n+m$ and of class 2. There are exactly $\tau(n, m, \mathbb{F}_3)$ such HGEC that are centrally irreducible.*

By counting every time the only entropic HGEC, one recovers the following previously known facts: there are up to isomorphism:

- just two 3^4-order HGECs, since $1 + \alpha(3, 1, \mathbb{F}_3) = 2$,
- also just two 3^5-order HGECs, since $1 + \alpha(4, 1, \mathbb{F}_3) = 2$ (recall that $\tau(4, 1, \mathbb{F}_3) = 0$),
- exactly four 3^6-order HGECs, since $1 + \alpha(4, 2, \mathbb{F}_3) + \alpha(5, 1, \mathbb{F}_3) = 1 + 1 + 2 = 4$; this follows from $\tau(4, 2, \mathbb{F}_3) + \tau(5, 1, \mathbb{F}_3) = 1 + 1 = 2$.

More generally, we are in a position to state:

Theorem 3.18. *For any $s \geq 4$ the number $H_2(s)$ of non isomorphic 3^s-order class 2 HGECs (or: class 2 exponent 3 CMLs) satisfies the following equality:*

$$H_2(s) = 1 + \sum_{4 \leq n \leq s-1} \alpha(n, s-n, \mathbb{F}_3).$$

The total number of 3^s-order HGECs coincides with $H_2(s)$ for $s \leq 7$, but otherwise it is bounded from below by $3 + H_2(s)$.

Proof: The sum-decomposition of $H_2(s)$ is nothing else than an easy consequence of a counting principle, each term $\alpha(n, s-n, \mathbb{F}_3)$ representing the subfamily of the HGECs whose rank is $n+1$. The rest follows from [6].

□

Corollary 3.19. *There are at least forty six* HGECs *of order* 3^8.

Proof: There are three class 3 exponent 3 CMLs, see [6] and $H_2(8) = 1 + \alpha(4,4,\mathbb{F}_3) + \alpha(5,3,\mathbb{F}_3) + \alpha(6,2,\mathbb{F}_3) + \alpha(7,1,\mathbb{F}_3) \geq 1+1+17+13+11 = 43$, since we just know lower bounds for: $\alpha(5,3,\mathbb{F}_3) \geq 17$ and for $\alpha(6,2,\mathbb{F}_3) \geq 13$. □

exp CMLs & HGECs \ order	3^4	3^5	3^6	3^7	3^8
rank 3 exp.3 CML or rank 4 HGECs	τ=1 α'=0 α(3,1)=1	0	0	0	0
rank 4 exp.3 CMLs or rank 5 HGECs	τ=0 α'=1 α(4,0)=1	$\searrow$ τ=1 α'=0 α(4,1)=1	$\searrow$ τ=1 α'=0 α(4,2)=1	$\searrow$ τ=1 α'=0 α(4,3)=1	$\searrow$ τ=1+ \ 3 of class 3 α'=0 α(4,4)+3=4
rank 5 exp.3 CMLs or rank 6 HGECs	0	$\searrow$ τ=0 α'=1 α(5,0)=1	$\searrow$ τ=1 α'=1 α(5,1)=2	$\searrow$ τ=5 α'=1 α(5,2)=6	$\searrow$ $\tau \geq 16$ α'=1 α(4,3) $\geq$ 17
rank 6 exp.3 CMLs or rank 7 HGECs	0	0	$\searrow$ τ=0 α'=1 α(6,0)=1	$\searrow$ τ=3 α'=2 α(6,1)=5	$\searrow$ τ=7 α'=6 α(6,2) $\geq$ 13
rank 7 exp.3 CMLs or rank 8 HGECs	0	0	0	$\searrow$ τ=0 α'=1 α(7,0)=1	$\searrow$ τ=6 α'=5 α(7,1)=11
rank 8 exp.3 CMLs or rank 9 HGECs	0	0	0	0	$\searrow$ τ=0 α'=1 α(8,0)=1
Total number of isom . classes	2	2	4	13	at least 46

Table 3: The number of isomorphism classes

The known cardinal number of isomorphism classes of 3^s-order rank n exponent 3 CMLs (or 3^s-order rank $(n+1)$ HGECs) may be summarized in the table 3. Each cell corresponds to $\alpha(n, s-n, \mathbb{F}_3)$ (abbreviated in $\alpha(n, s-n)$) except for 3^8- order rank 5 HGECs, in which one must add three class 3 HGECs (see [2], [6], [8]). From our Theorem 3.1, each α is the sum $\alpha(n, s-n) = \tau + \alpha'$, where $\tau = \tau(n, s-n, \mathbb{F}_3)$ is the number of centrally irreducible CMLs or HGECs and $\alpha' = \alpha(n-1, s-1)$ which coincides with the value of α in the cell in position north-west. It is easier to determine first α' that represents the number of centrally reductible HGECs or CMLs. If one knows already all the $3^{(s-1)}-$ order HGECs, then one needs only to determine the centrally irreducible 3^s-order HGECs whose number is:

$$H_2(s) - H_2(s-1) = \textstyle\sum_{4 \leq n \leq s-1} \tau(n, s-n, \mathbb{F}_3).$$

This sum represents the number of those that are authentically new among the 3^s-order HGECs. Furthermore, our "alternative approach" is more than a counting device; it may be employed to provide explicit descriptions of small order HGECs.

For instance, we may say that there are up to isomorphism exactly thirteen order 3^7 HGECs (including the entropic one and twelve ones that are not entropic), since: $\alpha(6,1,\mathbb{F}_3)+\alpha(5,2,\mathbb{F}_3)+\alpha(4,3,\mathbb{F}_3)=5+6+1=12$. If we want to describe explicitly the rank 6 ones (whose number is $\alpha(5,2,\mathbb{F}_3)=6$), we must start from any representative of $\mathrm{AT}(5,2,\mathbb{F}_3)$. As a case in point, let us construct the HGEC whose factorized associator is $t_2=(e_{123}=e_{145};e_{245})$. Consider $V=V(5,\mathbb{F}_3)$ and the subspace W of Λ^3V spanned by $e_{123}-e_{145}$ and by all the e_{ijk} such that $i<j<k$ with $(i,j,k)\neq(2,4,5)$, $(1,2,3)$ and $(1,4,5)$.

Thus $W=\Lambda^3V/R$ is generated by $u=\overline{e_{123}}$ and $v=\overline{e_{245}}$. The sum $E=V\bigoplus W$ is 7-dimensional.

Our process yields a rank 5 exponent 3 CML of order 3^7 whose factorized associator is

$$\delta(\overline{x},\overline{y},\overline{z})=(e^*_{123}+e^*_{145})(\overline{x},\overline{y},\overline{z}).u+e^*_{234}(\overline{x},\overline{y},\overline{z}).v,$$

For any two vectors x and y from E, the binary law of the loop is defined by

$$x*y=x+y+(x_2y_3-x_3y_2+x_4y_5-x_5y_4)(x_1-y_1).u+(x_3y_4-x_4y_3)(x_2-y_2).v.$$

Besides, $(E(t_2),*)$ can be viewed as the free exponent 3 CML on five generators submitted only to the following relations: $(\Delta(e_1,e_2,e_3)-\Delta(e_1,e_4,e_5))=e=\Delta(e_i,e_j,e_k)$ for any $i<j<k$ with $(i,j,k)\neq(2,4,5),(1,2,3)$ and $(1,4,5)$. The other CMLs $(E(t_i),*)$ can be similarly described in terms of generators and relations. Now, since $\tau(7,1,\mathbb{F}_3)=6$ and $\alpha(6,1,\mathbb{F}_3)=5$, we may derive the following new classification result:

Theorem 3.20. *There are exactly eleven rank* 8 HGECs *whose* 3*-order is* 8*, and among them only* 6 *are centrally irreducible and admit as factorized associators one of the previously defined alternate trilinear forms:* f_5,f_6,f_7,f_8,f_9 *and* $(e^*_{147}+g_{(-1)})$.

Several papers have been devoted to descriptions of important and somewhat complicated finite groups by using their connection with some Moufang loops (see [11] and its bibliography). Now we have already described as the third example in Section 1 the HGEC and the exponent 3 CML whose factorized associator is f_9. The subgroups of the linear groups preserving all the forms f_i are known (see Cohen and Helminck [9]). We deduce the following fact:

Theorem 3.21. *The* GEC $E(f_9)$ *has an automorphism group* Γ *that is an extension of* $G_2(\mathbb{F}_3)$ *(Chevalley's group of type* G_2 *over* $\mathbb{F}_3$*). The related* CML *has rank* 7 *and exponent* 3*; it has an automorphism group* $A=\mathrm{Aut}(E(f_9),*)$ *such that there exists a splitting exact sequence of the form*

$$0\to\mathbb{Z}_3^7\longmapsto A=\mathrm{Aut}(E(f_9),*)\overset{\Psi}{\twoheadrightarrow}G(f_9)\longrightarrow 0.$$

Here Ψ *is the canonical morphism from* A *onto the stabilizer* $G(f_9)$ *of* f_9 *in the linear group* $\mathrm{GL}(7,\mathbb{F}_3)$*. Besides,* $G(f_9)$ *is isomorphic to some product of the form* $\{\pm1\}.G_2(\mathbb{F}_2)$*; and we have* $\ker\Psi\simeq\mathbb{Z}_3^7$ *and* $|\Gamma|=3^8.\,|A|=2.3^{15}.\,|G_2(\mathbb{F}_3)|$.

Concluding remarks:

Our transfer theorem provides a link between two classification problems. Any advance in the classification of finite HGECs or exponent 3 CMLs is thereby related to an eventual progress in the classification of alternate trilinear mappings up to changes of basis. This last problem is understandable by anyone who has an elementary mathematical background. But it is not altogether easy to continue the classification. The determination of $\alpha(8,1,\mathbb{F}_q)$ seems to be rather difficult, even in case $q=3$. Likewise, exact estimations of $\alpha(6,2,\mathbb{F}_q)$ and $\alpha(5,3,\mathbb{F}_q)$ cannot be obtained as long as significative invariants are not found. Another direction for further investigations concerns the class 3 exponent 3 CMLs. Though we were able to describe completely all these loops when their order is minimum (3^8), we did not provide a general exterior algebra description for them (see nevertheless [8] and [4] for the free objects $L_{(n,3)}$).

It would be nice also to extend Schwenk's correspondence theorem so as to get a classification up to isomorphism of the GECs related to a given 3-power order CML $(G,+)$. The number of non isomorphic GECs of the form (G,T_c) depends obviously on the action of $\mathrm{Aut}(G,+)$ on the center Z, since (G,T_c) is isomorphic to (G,T_d), as soon as $d=f(c)+3t$ with $f\in\mathrm{Aut}(G,+)$ and $t\in Z$. Anyway the situation is doubtless more complicated than for abelian 3-groups.

Besides, an exhaustive classification of the order 9 GECs seems to be a rather tedious task. Of course, there are only four such terentropic (or entropic) GECs, and one may find elliptic curves whose related groups are $\mathbb{Z}_9$ or $\mathbb{Z}_3\times\mathbb{Z}_3$. But an algebraic approach of the non entropic one is not so easy.

We have already mentioned that the groups $(P,*)$ arising from finite elliptic curves are used for implementing public-key cryptosystems. The best-know protocol that is used then for coding secret messages m from P is the ElGamal protocol that consists in sending pairs of elements from P of the form $C(m)=(m*B^r;g^r)=(\mu;\delta)$ where B and g, as well as the initial group $(P,*)$ are made public by the owner of the mailbox, while r is an arbitrary integer whose choice is made at random by the sender (S). Clearly, $\mu=m*B^r$ is a masked message that S sends with a key $\delta=g^r$. The recipient R is supposed to know a secret function σ such that $\sigma(g^r)=(B^r)^{-1}$. Thus R may decrypt and recover the initial message by: $\mu*\sigma(\delta)=m$, since $(m*B^r)*(B^r)^{-1}=m$.

Usually, σ has the form: $\sigma(g^r)=g^{rl}$, where the exponent l is a secret integer, and the elements from the cyclic group $\langle g\rangle$ are written so that a computation of l such that $g^l=B$ be infeasible. This has been the case for large cyclic group $\langle g\rangle$ in the multiplicative group $\mathbb{F}_q^*$, considering the $\mathbb{Z}_p$-vector representation of its elements, where p is the characteristic. But subexponential algorithms are available by now for computing l, so one employs elliptic curve groups in order to recover the same level of security. An alternative would be to use large cyclic subgroups contained in di-associative loops $(E,*)$, since the recovering of the initial message by: $(m*B^r)*(B^r)^{-1}=m$ is still valid.

References

[1] Abou Hashish M., *Applications trilinéaires alternées et courbes cubiques elliptiques généralisées classifications et utilisations cryptographiques*, Thèse de Doctorat, no. 687, Institut National des Sciences Appliquées de Toulouse, 2003.

[2] Bénéteau L., *Ordre minimum des boucles de Moufang commutatives de classe* 2 (*resp.* 3), Ann. Fac. Sci. Toulouse Math. (5) **3** (1981), 75–88.

[3] Bénéteau L., *Extended triple systems: geometric motivations and algebraic constructions*, Discrete Math. **208/209** (1999), 31–47.

[4] Bénéteau L., Kepka P., *Quasigroupes trimédiaux et boucles de Moufang commutatives libres*, C.R. Acad. Sci. Paris, t. 300, Série I, no. 12 (1985), 377–380.

[5] Bénéteau L., Lacaze J., *Symplectic trilinear form and related designs and quasigroups*, Comm. Algebra **16** (5) (1988), 1035–1051.

[6] Bénéteau L., Razafimanantsoa G., *Boucles de Moufang k-nilpotentes minimales*, C.R. Acad. Sci. Paris, Série I **306** (1988), 743–746.

[7] Buekenhout F., *Generalized elliptic cubic curves*, Part 1, Finite Geometries, (2001), 35–48.

[8] Chein O., Pflugfelder H.O., Smith J.D.H., *Quasigroups and Loops; Theory and Applications*, Sigma Series in Pure Mathematics, vol. 8, Heldermann, Berlin, 1990.

[9] Cohen A., Helminck A., *Trilinear alternating forms on a vector space of dimension* 7, Comm. Algebra **16.1** (1988), 1–25.

[10] Djokovic D.Z., *Classification of* 3*-vectors of a real* 8*-dimensional vector space*, Linear and multilinear algebra (1983), 3–39.

[11] Griess R.L., Jr., *A Moufang loop, the exceptional Jordan algebra, and a cubic form in* 27 *variables*, J. Algebra **131** (1990), no. 1, 281–295.

[12] Gurewitch G.B., *Foundations of the Theory of Algebraic Invariants*, P. Noordhoff LTD, Groningen, Netherlands, 1964.

[13] Keedwell A.D., *More simple constructions for elliptic cubic curves with small numbers of points*, Pure Math. Appl. Ser. A, Vol. 3, No. 3–4, (1992), 199–214.

[14] Kepka T., Němec P., *Commutative Moufang loops and distributive groupoids of small orders*, Czechoslovak Math. J. **31** (106) (1981), 633–669.

[15] Kepka T., *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolinae **17** (1976), 229–240.

[16] Koblitz N., *A course in Number Theory and Cryptography*, Second Edition, New-York, Springer-Verlag, 1994.

[17] Manin Yu.I., *Cubic Forms, Algebra, Geometry, Arithmetic*, North-Holland, Amsterdam, London, 1974.

[18] Němec P., *Commutative Moufang loops corresponding to linear quasigroups*, Comment. Math. Univ. Carolinae **29** (1988), 303–308.

[19] Noui L., *Formes multilinéaires alternées*, Thèse de troisième cycle, Université de Montpellier II, 1995.

[20] Razafimanantsoa G., *La k-nilpotence minimale dans les boucles de Moufong commutatives; classification partielle des applications trilinéaires alternées*, Thèse no. 3511, Univ. Toulouse III, 1988.

[21] Revoy Ph., *Fomes trilinéaires alternées de rang* 7, Bull. Sci. Math. 2^e112, (1988), 357–368.

[22] Schoof R., *Counting points on elliptic curves over finite fields*, Journal de Théorie des nombres de Bordeaux VII, (1995), 219–254.

[23] Schouten J.A., *Klassifizierung der alternierender Grössen dritten Grades in* 7 *Dimensionen*, Rend. Circ. Nat. di Palermo **55** (1931), 137–156.

[24] Schwenk J., *A classification of abelian quasigroups*, Rend. Math. Appl. (7) **15** (2) (1995), 161–172.

[25] Smith J.D.H., *Finite equationally complete entropic quasigroups*, Contribution to General Algebra, Proc. Klagenfurt Conf., 1978 pp. 345–355.

[26] Vinberg E.B., Elasvili A.G., *Classification of trivectors of a nine-dimensional space*, Trudy Sem. Vekt. Tenz. Analizu, no. XVIII, (1978), 197–223.

[27] Westwick R., *Real trivectors of rank seven*, Linear and Multilinear Algebra (1980), 183–204.

GMM INSA, 135 Avenue de Rangueil, 31077 Toulouse, France

E-mail: hashish@gmm.insa-tlse.fr
beneteau@gmm.insa-tlse.fr

(*Received* October 3, 2003, *revised* March 15, 2004)