Check character systems using Chevalley groups

Claudia Broecker, Ralph-Hardo Schulz and Gernot Stroth

Dedicated to Prof. Dr. Hanfried Lenz on occasion of his 80^{th} birthday

Abstract: We show that the Sylow 2-subgroups of nearly all Chevalley groups in even characteristic allow the definition of a check-character-system which detects all single and the most important double errors.

Key words: check character system, check digit system, error detecting code, Suzuki-2-groups, fixed-point-free automorphisms, p-groups, Chevalley groups

0. Introduction

Defining a check character system over a finite group using one of its automorphisms, we derive the necessary conditions for the detection of the most frequent errors (cf. [?], [?]). In the abelian case, there are many groups fulfilling these conditions ([?]). Here, we give examples for the non-abelian case; indeed the Sylow-2-groups of nearly all Chevalley groups can be used for the construction of such a check character system.

1. The Problem

Definition 1 :*Check-character-system* ([?])
Let $(G, \cdot)$ be a finite group and $\delta_1, ..., \delta_n$ permutations of the set G. Then a *check character system* on the alphabet G (defined implicitely) is given by $G^{n-1} \to G^n$ with $g_1...g_{n-1} \mapsto g_1...g_{n-1}g_n$ where the *check character* g_n is determined from the *information digits* by the *check equation*

$$\prod_{i=1}^{n} \delta_i(g_i) = 1.$$

In this article we put $\delta_i := T^i$ for a fixed automorphism T of the group G.

In tabular 1 we give a list of the most important errors (cf. [?]) and state sufficient conditions on the automorphism T for the detection of these errors. For $n \geq 4$ the conditions are also necessary.

Tabular 1

	Type	Conditions on T (for all $a, y \in G$, $a \neq 1$)
1.	$g_1 ... g_i ... g_n \rightsquigarrow g_1 ... g_i' ... g_n$	none
2.a)	$g_1 ... g_i g_{i+1} ... g_n \rightsquigarrow g_1 ... g_{i+1} g_i ... g_n$	$T(a) \neq y^{-1}ay$
b)	$... g_i g_{i+1} g_{i+2} ... \rightsquigarrow ... g_{i+2} g_{i+1} g_i ...$	$T^2(a) \neq y^{-1}ay$
3.a)	$... g_i b b g_{i+3} ... \rightsquigarrow ... g_i b' b' g_{i+3} ...$	$T(a) \neq y^{-1}a^{-1}y$
b)	$... b g_i b ... \rightsquigarrow ... b' g_i b' ...$	$T^2(a) \neq y^{-1}a^{-1}y$

Proof . Consider e.g. type 2.a). The error is detected iff $T^i(g_i)T^{i+1}(g_{i+1}) \neq T^i(g_{i+1})T^{i+1}(g_i)$ which is equivalent to $T(g_{i+1}g_i^{-1}) \neq g_i^{-1}(g_{i+1}g_i^{-1})g_i$. The other conditions follow in the same way. $\square$

Definition 2: Let G be a finite group. An automorphism T of G is called *good* provided for all $x \in G, x \neq 1$ we have

$$\begin{array}{ll} (i) & x^T \text{ is not conjugate to } x \text{ or } x^{-1} \text{ in } G \\ (ii) & x^{T^2} \text{ is not conjugate to } x \text{ or } x^{-1} \text{ in } G \end{array}$$

We are going to show that there are many groups G possessing a good automorphism.

Remarks: 1.) If G is abelian, then T satisfies the conditions 1, 2.a), 2.b) and 3.a) if T^2 is fixed-point free on G and T is good if T^4 is fixed-point free.
2.) Note that for any group G and automorphism T of odd order t already condition 2a) implies that T is good:
Since $gcd(4, t) = 1$ there exist integers r and s with $4r + st = 1$; therefore, any conjugate class fixed by T^4 must be fixed by $T = T^{4r+st}$ too.

2. A first example

We consider the following group in the non-abelian case: The set Q of matrices of the type

$$(x, y) := \begin{pmatrix} 1 & x & y \\ 0 & 1 & x^q \\ 0 & 0 & 1 \end{pmatrix}$$

with $x, y \in GF(q^2)$, $q = 2^m > 2$ and $y + y^q + x^{q+1} = 0$ and its automorphisms induced by conjugation with

$$H_\lambda := \begin{pmatrix} \lambda^{-q} & 0 & 0 \\ 0 & \lambda^{q-1} & 0 \\ 0 & 0 & \lambda \end{pmatrix} \quad (\lambda \in GF(q^2)^\star)$$

form a Suzuki-2-group of type B ([?], cf. [?] pp 314-315).

Proposition 1
Let Q be the Suzuki-2-group of order q^3 defined above. Then the automorphism $T : (x, y) \mapsto (x\lambda^{2q-1}, y\lambda^{q+1})$ is a good automorphism if the multiplicative order of λ is not a divisor of $(q + 1)$.

Proof . Let $\overline{(x, y)}$ denote the conjugacy class of an element (x, y) of Q. Then $\overline{(x, y)} = \{(x, y + xa^q + x^q a) : (a, b) \in Q\}$ and $\overline{(x, y)^{-1}} = \{(x, y^q + xa^q + x^q a) : (a, b) \in Q\}$. To fulfill condition 2.a) it is sufficient to have $\lambda^{q+1} \neq 1$ for the involutions $(0, y)$ with $y \in GF(q)$ and $\lambda^{2q-1} \neq 1$ otherwise. But $\lambda^{2q-1} = 1 = \lambda^{q^2-1}$ means that the multiplicative order of λ is 3 in which case the two conditions are equivalent. Since $o(\lambda)$ is odd we can use Remark 2 from section 1. □

Corollary
The check character system defined over the Suzuki-2-group Q using the automorphism T of order $q-1$ detects all single errors, neighbour-transpositions, twin errors, jump-transpositions and jump-twin-errors.

3. Good automorphisms on p-groups

The following Lemma shows that it is not possible to classify even the p-groups admitting a good automorphism.

Lemma 1:
Let P be a p-group and $\alpha \in Aut(P)$. Suppose $gcd(o(\alpha), p(p-1)) = 1$. Then α is good if and only if α is fixed point free on P.

Proof . There exists an α-invariant chain $P_o = 1 < P_1 < \ldots < P_n = P$ of normal subgroups of P such that P_i/P_{i-1} is elementary abelian and $[P, P_i] \subseteq P_{i-1}$ for $i = 1, \ldots, n$: Take for instance $P_1 := \Omega_1(Z(P))$ and define P_i inductively such that $P_i/P_{i-1} = \Omega_1(Z(P/P_{i-1}))$. (Here $\Omega_1(G)$ denotes the subgroup of G generated by the elements of order p).

Suppose first that α acts fixed point freely on P. Then α acts fixed point freely on each P_i/P_{i-1} (cf. [?] p 335).
Choose $x \in P$ such that x^α is conjugate in P to x. Let i be minimal with $x \in P_i$. Suppose $i > 0$. Then $x \notin P_{i-1}$ and so $x^\alpha \in P_i \setminus P_{i-1}$. Now $(xP_{i-1})^\alpha$ is conjugate to xP_{i-1}. As $x^{-1}x^P \subseteq [P_i, P] \subseteq P_{i-1}$ we have $x^P \subseteq xP_{i-1}$. Hence $\langle xP_{i-1}\rangle^\alpha = \langle xP_{i-1}\rangle$. As $\mathrm{Aut}(\langle xP_{i-1}\rangle)$ is cyclic of order $p-1$, and $gcd(o(\alpha), p-1) = 1$, we see $(xP_{i-1})^\alpha = xP_{i-1}$, which contradicts the fact that α acts fixed point freely on P_i/P_{i-1}. Hence $i = 0$ and so $x = 1$. As $o(\alpha)$ is odd we can apply Remark 2 of section 1 and see that α is good.

If α is good, then by definition α acts fixed point freely on P. $\square$

Proposition 2: *Let $G \cong L_2(q), q = 2^m, m > 1$, and $S \in Syl_2(G)$. Then for every u with $u|(q-1), u \neq 1$ there is some $\alpha \in G$ of order u, such that α induces a good automorphism on S.*

Proof . We have

$$S = \{ \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \Big| v \in GF(q) \ \} \quad \text{and} \quad T = \{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \Big| x \in GF(q)^* \}$$

Let $t \in T, t \neq 1$.Then t acts fixed point freely on S. As $o(t)$ is odd, the assertion follows with Lemma 1. $\square$

Proposition 3: *Let $G \cong U_3(q), q = 2^m > 2$, and $S \in Syl_2(G)$. Then for every u with $u|(q-1), u \neq 1$ there is some $\alpha \in G$ of order u, such that α induces a good automorphism on S.*

Proof . S is of the form considered in section 2. $\square$

Proposition 4: *Let $G \cong Sz(q), q = 2^{2m+1} > 2$, and $S \in Syl_2(G)$, furthermore $1 \neq u|(q-1)$. Then there is some $\alpha \in G$ of order u, such that α induces a good automorphism on S.*

Proof . Defining $x^{\pi} := x^{2^{m+1}}$, we have (cf. [?] pp 182-184) without loss of generality

$$S = \{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a^{\pi} & 1 & 0 \\ a^{2+\pi} + ab + b^{\pi} & a^{\pi+1} + b & a & 1 \end{pmatrix} \mid a, b \in GF(q) \}$$

and

$$T = \{ \begin{pmatrix} \lambda^{1+2^m} & 0 & 0 & 0 \\ 0 & \lambda^{2^m} & 0 & 0 \\ 0 & 0 & \lambda^{-2^m} & 0 \\ 0 & 0 & 0 & \lambda^{-1-2^m} \end{pmatrix} \mid \lambda \in GF(q)^{\star} \}$$

Then $|T| = (q-1)$ and T acts fixed point freely on S. The assertion follows with Lemma 1. $\square$

From the propositions 2, 3 and 4 we get:

Result 1:
The Sylow 2-subgroups of $L_2(q)$, $Sz(q)$ and $U_3(q)$ with $q = 2^m$ are examples of groups which admit a good automorphism.

Corollary
The groups mentioned in Result 1 admit a check character system which detects all single errors, neighbour-transpositions, twin errors, jump transpositions and jump-twin-errors.

Result 2:
Let S be a Sylow 2-subgroup of a Chevalley group (twisted or not) over $GF(q), q = 2^m$. Then there is some $\alpha \in G$ such that α induces a good automorphism α of S with $o(\alpha)|(q-1)$, provided q is large enough.

Sketch of the proof. (The details can be worked out easily by the interested reader.) The main idea is to prove the assertion by an induction to the Lie rank. The statement is true for the groups of Lie rank 1, i. e. $L_2(q), Sz(q)$ and $U_3(q)$, see Result 1. All Lie groups possess a maximal parabolic H such that $H/O_2(H)$ possesses a normal subgroup K which is a Lie group of smaller rank, $|H/O_2(H) : K|$ is odd and K is centralized by a cyclic group T of order $(q-1)/d$, where $d = 1, 3$ or $d = gcd(n, q-1)$ in case $G \cong L_n(q)$ (see $[Ca]$ for details). Let $T = \langle\beta\rangle$. Then β^i acts fixed point freely on $O_2(H)$ for $\beta^i \neq 1$(cf. [?]). By induction on the Lie rank there is some $\gamma \in K$, with $o(\gamma)|(q-1)$, such that γ induces a good automorphism on $S/O_2(H), S \in \mathrm{Syl}_2(G)$.

As any K-composition factor in $O_2(H)$ is a module over $GF(q)$ we get that γ is diagonizable. Suppose q is large enough, then there is a power β^i such that β^i does not share any eigenvalue with γ on the modules of K in $O_2(H)$. Set $\alpha = \gamma\beta^i$. Then α acts fixed point freely on S. The conclusion follows with Lemma 1. $\square$

The result is also true for Sylow p-subgroups of Chevalley groups over $GF(p)$, p odd. For example the Sylow 3-subgroup of $L_3(3^3)$ possesses a good automorphism α of order 13.

We will conclude this paper with some general
Remarks. 1.) If a group G possesses a good automorphism of prime order, then by a result of J. Thompson [Go, 10.2.1] G is nilpotent. So the Sylow groups are characteristic and we can apply Lemma 1.
2.) If G possesses a good automorphism α with $gcd(o(\alpha), |G|) = 1$ then by [Ro] G is solvable. For solvable groups a similar lemma as Lemma 1 holds if $gcd(o(\alpha), |G|\varphi(|G|)) = 1$ as one can derive by analyzing $G \cdot \langle\alpha\rangle$. But this condition is not necessary for the existence of a good automorphism, as can be seen from the following.
3.) Let N be the additive group of the 3-dimensional vector space K^3 over $K = GF(8)$; then N is elementary abelian of order 2^9. We see that N admits the linear mappings with matrices from

$$T = \{\begin{pmatrix} a & & O \\ & a^2 & \\ O & & a^4 \end{pmatrix} |a \in GF(8)^\star\} \leq SL_3(8),$$

furthermore the automorphisms $\bar{\gamma}$ and $\bar{\beta}$ with matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b & & O \\ & b & \\ O & & b \end{pmatrix} = b\, \mathrm{I}_3$$

(for a fixed $b \in GF(8) \setminus \{0,1\}$) respectively. Let $G = TN$ be the semidirect product of T and N, defined by $(t_1, n_1)(t_2, n_2) = (t_1 \cdot t_2, n_1^{t_2} + n_2)$.
Now G, a group of order $7 \cdot 2^9$, is soluble but not nilpotent. Any automorphism $\bar{\xi}$ of N normalizing T can be extended to an automorphism ξ of G by defining $(t,n)^\xi := (\bar{\xi}^{-1}\, t\, \bar{\xi}, n^{\bar{\xi}})$. So, from $\bar{\gamma}$ and $\bar{\beta}$, one gets automorphisms γ and β of order 3 and 7.
Since γ and β commute, $\alpha := \beta\gamma$ is an automorphism of order 21 of G. Assume that α is not good. By remark 2 of section 1 we can assume without loss of generality that there exists an element $x \in G^\star$ which is conjugate to x^α. Let $(t,n)^\alpha = (s,m)^{-1}(t,n)(s,m)$. Since $\bar{\gamma}^{-1} t \bar{\gamma} = t^2$ we see that $t^2 = t = id$ and $bn^{\bar{\gamma}} = n^s$. But this equation holds only for $n = 0$ or $b^3 = b = 1$, a contradiction.
So we have found a good automorphism α of the group G with

$$gcd(o(\alpha), |G|) = gcd(21, 7 \cdot 2^9) \neq 1\,.$$

References

[Ca] R. Carter, Simple groups of Lie type, Wiley 1972

[Go] D. Gorenstein, Finite groups, Harper and Row 1968

[Hi] Higman,G., Suzuki-2-Groups, Illinois J. Math. 7, pp 79-96 (1963)

[Hu1] Huppert,B. & N.Blackburn, Finite Groups II, Berlin etc. Springer V. (1982)

[Hu2] Huppert, B. & N.Blackburn, Finite Groups III, Berlin etc. Springer V. (1982)

[Ro] P. Rowley, Finite groups admitting a fixed point free automorphism group, J. Algebra, to appear

[S1] Schulz,R.-H., Codierungstheorie ,Vieweg Verlag, pp 58-62 (1991)

[S2] Schulz,R.-H., Check character systems over groups and orthogonal Latin squares, Applic. Algebra in Eng., Comm. and Computing, AAECC, to appear

[Ve] Verhoeff,J., Error Detecting Decimal Codes, Math.Centre Tracts 29, Math. Centrum Amsterdam (1969)

Claudia Broecker,
Ralph-Hardo Schulz
2. Mathematisches Institut
Freie Universität Berlin
Arnimallee 3
D-14195 Berlin
e-mail: schulz@math.fu-berlin.de
or broecker@math.fu-berlin.de

Gernot Stroth
Martin-Luther-Universität
Halle-Wittenberg
Fachbereich Mathematik und Informatik
Institut für Algebra und Geometrie
D-06099 Halle
e-mail:
stroth@coxeter.mathematik.uni-halle.de