Astérisque

REINHARD KNÖRR

WOLFGANG WILLEMS

The automorphism groups of generalized Reed-Muller codes

Astérisque, tome 181-182 (1990), p. 195-207

<http://www.numdam.org/item?id=AST_1990__181-182__195_0>

The Automorphism Groups of Generalized Reed-Muller Codes

Reinhard Knörr and Wolfgang Willems

1. Introduction

The generalized Reed-Muller Codes of length p^m over the prime field $\mathbb{F}_p$ are the radical powers $J(\mathbb{F}_pE)^r$ $(0 \leq r \leq m(p-1))$ of the group algebra $\mathbb{F}_pE$ of an elementary abelian p-group E of rank m. To be consistent with the notation in the literature we put

$$GRM(r,m) = J(\mathbb{F}_pE)^{m(p-1)-r} \quad (0 \leq r \leq m(p-1)) .$$

Then $GRM(r,m)$ is the r-th order generalized Reed-Muller Code of length p^m over $\mathbb{F}_p$.

In an earlier paper [4] we characterized such codes as those linear codes of length p^m over $\mathbb{F}_p$ which contain the affine general linear group $AGL(m,p)$ as a subgroup of their automorphism group.

In the binary case the automorphism group of a generalized Reed-Muller Code - which is the original Reed-Muller Code [6] - has been known for a long time ([5], Chap. 13, §9). Here we prove

S.M.F.
Astérisque 181-182 (1990)

<u>Theorem</u>. For any prime p we have

$$\mathrm{Aut}(\mathrm{GRM}(r,m)) = \begin{cases} \text{The full monomial group if } r = m(p-1) \\ \mathbb{F}_p^* \times S_{p^m} \quad \text{if } r = 0,\ m(p-1)-1 \\ \mathbb{F}_p^* \times \mathrm{AGL}(m,p) \quad \text{otherwise.} \end{cases}$$

Although the result does not depend on whether the prime p is odd or even, the proofs are rather different in the two cases. The difference lies in the fact that only in the binary case a nice geometrical interpretation of the code is available ([5] Chap. 13, §4), from which the crucial point

$$\mathrm{Aut}(\mathrm{RM}(r,m)) \subseteq \mathrm{Aut}(\mathrm{RM}(r+1,m)) \quad (0 < r \leq m-1)$$

in the proof ([5], Chap. 13, §9) follows. This fails in odd characteristic. The proof we present here heavily depends on the classification of doubly transitive groups.

2. Proof of the Theorem

Let V be a vector space over the field F with basis $\{v_1,\dots,v_n\}$ and let C be a linear code in V. If $g \in \mathrm{Aut}(C)$ then g defines a permutation $\pi = \pi_g \in S_n$ such that

$$v_i g = f_i v_{i\pi} \quad (f_i \in F^*,\ i = 1,\dots,n)\ .$$

Thus there is a homomorphism

$$\alpha : \mathrm{Aut}(C) \longrightarrow S_n$$
$$g \longrightarrow \pi_g$$

and if $P\,\mathrm{Aut}(C)$ denotes the image of α we obtain an exact sequence

(<u>A</u>) $$1 \to D(\mathrm{Aut}(C)) \to \mathrm{Aut}(C) \xrightarrow{\alpha} P\,\mathrm{Aut}(C) \to 1$$

where the kernel $D(\mathrm{Aut}(C))$ of α consists of the diagonal automorphisms of $\mathrm{Aut}(C)$.

For the reader's convenience we restate the following well known result:

Lemma 1 [3]. If C is non-trivial (i.e. $0 \lneqq C \lneqq V$) and if $P\,\mathrm{Aut}(C)$ acts doubly transitively on the coordinate positions then $D(\mathrm{Aut}(C)) = F^{*}\cdot \mathrm{id}$.

Proof. Let $0 \neq c = a_1\upsilon_1 + \ldots + a_n\upsilon_n \in C$ with $w(c)$ minimal where w denotes the weight functions on V and $a_i \in F$. Obviously $w(c) \geq 2$ as $P\,\mathrm{Aut}(C)$ acts transitively and C is nontrivial. Now suppose that $d \in D(\mathrm{Aut}(C))$ with

$$\upsilon_i d = f_i \upsilon_i \quad (i = 1,\ldots,n)$$

where $f_i \in F^{*}$ and $f_n \neq f_{i_0}$ for a suitable i_0. As the action of $P\,\mathrm{Aut}(C)$ even is doubly transitive we may assume that $a_n \neq 0 \neq a_{i_0}$. It follows

$$C \ni f_n c - cd = \sum_{i=1}^{n} (f_n - f_i) a_i \upsilon_i$$

with $(f_n - f_{i_0}) a_{i_0} \neq 0$ and $w(f_n c - cd) < w(c)$, a contradiction.

As already mentioned, $AGL(m,p)$ is contained in the automorphism group of $GRM(r,m)$ for each r. If we write $AGL(m,p) = E \rtimes GL(m,p)$ then E acts by right multiplication and $GL(m,p)$ by conjugation on $\mathbb{F}_pE$ and therefore on all the radical powers $J(\mathbb{F}_pE)^r$. This action is doubly transitive on the coordinate positions. Then

$$(\underline{B}) \qquad D(GRM(r,m)) = \mathbb{F}_p^{*}$$

by Lemma 1, provided $r < m(p-1)$.

Lemma 2. $\mathrm{Aut}(GRM(r,m)) = \mathbb{F}_p^{*} \times S_{p^m}$ for $r = 0$ and $m(p-1)-1$.

Proof. Obviously, S_{p^m} is contained in the automorphism group of the socle of $\mathbb{F}_pE$ and the radical $J(\mathbb{F}_pE)$. The assertion follows now immediately from (A) and (B).

Lemma 3. $\mathrm{Aut}(\mathrm{GRM}(1,m)) = \mathrm{Aut}(\mathrm{GRM}(m(p-1)-2,m) = \mathbb{F}_p^* \times \mathrm{AGL}(m,p)$ for $m(p-1)-2 \geq 0$.

Proof. Since $\mathbb{F}_pE$ is a uniserial $\mathbb{F}_p\mathrm{AGL}(m,p)$-module (see [4]), $\mathrm{GRM}(1,m)$ is the orthogonal of $\mathrm{GRM}(m(p-1)-2,m)$. Thus, by duality, it is sufficient to prove the second equality. Let $J^2 = J(\mathbb{F}_pE)^2 = \mathrm{GRM}(m(p-1)-2,m)$ and let $g \in \mathrm{Aut}(J^2)$. If $x = \sum_{e\in E} a_e e \in \mathbb{F}_pE$ then $xg = \Sigma\, a_e g(e)(e\pi_g)$ where $g(e) \in \mathbb{F}_p^*$ and π_g is a permutation of E . Via a transformation with a suitable element of $\mathbb{F}_p^* \times \mathrm{AGL}(m,p)$ we may assume that $1g = 1$. Now let $x = (e-1)(e'-1) = ee'-e-e'+1 \in J^2$ with $e,e' \in E$. Thus $xg = g(ee')(ee')\pi_g - g(e)(e\pi_g) - g(e')(e'\pi_g)+1 \in J^2$. As $xg \in J^2$, we have

$$g(ee') - g(e) - g(e') + 1 = 0 .$$

In particular, for $e' = e^i$, this yields

$$g(e^{i+1}) = g(e) + g(e^i) - 1 .$$

Inductively, we obtain

$$g(e^i) = 1 + i(g(e) -1) .$$

If $g(e) \neq 1$ then there exists an $i \in \mathbb{N}$ with $1 \leq i \leq p-1$ such that $i(g(e) -1) = -1$, hence $g(e^i) = 0$, a contradiction. Thus $g(e) = 1$ for all $e \in E$. It follows

$$(ee')\pi_g - e\pi_g - e'\pi_g + 1 \in J^2$$

and obviously also

$$(e\pi_g)(e'\pi_g) - e\pi_g - e'\pi_g + 1 \in J^2 .$$

Thus

$$(e\pi_g)(e'\pi_g) - (ee')\pi_g \in J^2 .$$

With $a:= (ee')\pi_g$ and $b = (e\pi_g)(e'\pi_g)$ we obtain

$$a^{-1}(b-a) = a^{-1}b-1 \in J^2 .$$

Suppose $e_1 = a^{-1}b \neq 1$. Then choose $e_2,\dots,e_m$ such that $E = \langle e_1,\dots,e_m\rangle$. Now consider the two-dimensional $\mathbb{F}_pE$-module $M = \mathbb{F}_p m_1 \oplus \mathbb{F}_p m_2$ with the action

$$m_1e_1 = m_1+m_2 \ , \quad m_2e_1 = m_2$$
$$m_ie_j = m_i \quad (i = 1,2 \ ; \quad j = 2,\dots,m) \ .$$

It follows $M(e_1-1) \neq 0$ but $MJ^2 = 0$ since $\dim M = 2$. Therefore $a^{-1}b = 1$, i.e.

$$(ee')\pi_g = (e\pi_g)(e'\pi_g)$$

and $\pi_g \in GL(m,p)$.

This shows $\mathrm{Aut}(GRM(m(p-1)-2,m)) \leq \mathbb{F}_p^* \times AGL(m,p)$ and equality holds by a previous remark.

<u>Lemma 4</u>. $\mathrm{Aut}(GRM(r,1)) = \mathbb{F}_p^* \times AGL(1,p)$ for $1 \leq r \leq p-3$.

<u>Proof</u>. Put $E = \langle e\rangle$, $\alpha_{ij} = \binom{i}{j} \in \mathbb{F}_p$ and $\beta_{ij} = (-1)^{i+j}\alpha_{ij}$ for $i,j = 0,1,\dots,p-1$. Let $g \in \mathrm{Aut}(J^k)$ with $J^k = J(\mathbb{F}_pE)^k$ and $2 \leq k \leq p-2$. Then

$$e^ig = f_ie^{i\pi} \quad (0 \leq i \leq p-1)$$

where $f_i \in \mathbb{F}_p^*$ and π is a permutation of $\{0,\dots,p-1\}$. Again, as $\mathbb{F}_p^* \times AGL(1,p)$ is contained in the automorphism group of $GRM(r,1)$, we may assume that

$$1g = 1 \quad (\text{i.e. } f_0 = 1 \text{ and } 0\pi = 0)$$
$$\text{and } eg = f_1e \quad (\text{i.e. } 1\pi = 1) \ .$$

Now we have to show that $g = 1$ or equivalently by (<u>B</u>) $\pi = \mathrm{id}$. Note that $\{(e-1)^s \mid s \geq k\}$ is a basis for J^k and

$$(e-1)^sg = \sum_i \beta_{si}e^ig = \sum_i \beta_{si}f_ie^{i\pi}$$
$$= \sum_{i,j} \beta_{si}f_i\alpha_{i\pi,j}(e-1)^j \ .$$

Thus

(1) $$\sum_i \beta_{si}f_i\alpha_{i\pi,j} = 0 \quad \text{for all } s \geq k > j \ .$$

For an arbitrary t and $j < k$ we obtain

$$f_t\alpha_{t\pi,j} = \sum_i \delta_{ti} f_i\, \alpha_{i\pi,j} = \sum_{s,i} \alpha_{ts}\beta_{si} f_i \alpha_{i\pi,j}$$
$$= \sum_{\substack{i,s \\ s<k}} \alpha_{ts}\beta_{si} f_i \alpha_{i\pi,j}$$
$$= \sum_i \Big(\sum_{\substack{s \\ s<k}} \alpha_{ts}\beta_{si}\Big) f_i \alpha_{i\pi,j} \,.$$

We put

(2) $$\gamma_{ti} := \sum_{\substack{s \\ s<k}} \alpha_{ts}\beta_{si}$$

Obviously

$$\gamma_{ti} = 0 \quad \text{for} \quad i \geq k \,,$$

since then $\beta_{si} = 0$ for all $s < k$.

Therefore

(3) $$\sum_{\substack{i \\ i<k}} \gamma_{ti} f_i \alpha_{i\pi,j} = f_t \alpha_{t\pi,j}$$

for all t and all $j < k$.

If $t < k$ then $\gamma_{ti} = \delta_{ti}$ and (3) says really nothing. Thus only the following equations are relevant.

(4) $$\sum_{\substack{i \\ i<k}} (f_t^{-1}\gamma_{ti} f_i)\alpha_{i\pi,j} = \alpha_{t\pi,j} \quad \text{for } j < k \text{ and } t \geq k \,.$$

For t fixed, (4) is a system of k equations ($j = 0,\dots,k-1$) in the k variables $(f_t^{-1}\gamma_{ti} f_i)$ ($i = 0,\dots,k-1$) with coefficient matrix

$$A := (\alpha_{i\pi,j}) = \begin{pmatrix} \binom{0\pi}{0} & \binom{0\pi}{1} & \cdots\cdots & \binom{0\pi}{k-1} \\ \binom{1\pi}{0} & \binom{1\pi}{1} & \cdots\cdots & \binom{1\pi}{k-1} \\ \vdots & \vdots & & \\ \binom{(k-1)\pi}{0} & \binom{(k-1)\pi}{1} & \cdots & \binom{(k-1)\pi}{k-1} \end{pmatrix}$$

Now $\det A$ can be transformed - delete denominators and add columns to later columns - to the Vandermonde determinant

$$\det \begin{bmatrix} 1 & 0\pi & (0\pi)^2 & \cdots & (0\pi)^{k-1} \\ 1 & 1\pi & (1\pi)^2 & & (1\pi)^{k-1} \\ \vdots & \vdots & \vdots & & \\ 1 & (k-1)\pi & ((k-1)\pi)^2 & \cdots & ((k-1)\pi)^{k-1} \end{bmatrix} \neq 0 .$$

Therefore, we can solve (4) by Cramers's rule, i.e.

$$f_t^{-1}\gamma_{ti}f_i = \frac{\det A_i}{\det A} \tag{5}$$

where the matrix A_i is obtained from A if the i-th row is replaced by $(\alpha_{t\pi,0},\ldots,\alpha_{t\pi,k-1})$.

Clearly

$$\prod_{j=0}^{k-1} (j!)\det A = \prod_{\substack{r,s \\ r<s<k}} (s\pi - r\pi)$$

$$= \prod_{\substack{r<s<k \\ r,s\neq i}} (s\pi - r\pi) \prod_{r<i} (i\pi - r\pi) \prod_{r>i} (r\pi - i\pi)$$

and

$$\prod_{j=0}^{k-1} (j!)\det A_i = \prod_{\substack{r<s<k \\ r,s\neq i}} (s\pi - r\pi) \prod_{r<i} (t\pi - r\pi) \prod_{r>i} (r\pi - t\pi) .$$

Thus

$$f_t^{-1}\gamma_{ti}f_i = \prod_{\substack{r<k \\ r\neq i}} \frac{(r\pi - t\pi)}{(r\pi - i\pi)} . \tag{6}$$

Since $\begin{bmatrix} t \\ s \end{bmatrix} \begin{bmatrix} s \\ i \end{bmatrix} = \begin{bmatrix} t \\ i \end{bmatrix} \begin{bmatrix} t-i \\ s-i \end{bmatrix}$ for $t \geq s \geq i$ we obtain

$$\gamma_{ti} = \sum_{s<k} \alpha_{ts}\beta_{si} = \sum_{s<k} \begin{bmatrix} t \\ s \end{bmatrix} \begin{bmatrix} s \\ i \end{bmatrix} (-1)^{s+i}$$

$$= \begin{bmatrix} t \\ i \end{bmatrix} \sum_{s<k} \begin{bmatrix} t-i \\ s-i \end{bmatrix} (-1)^{s-i}$$

$$= \begin{bmatrix} t \\ i \end{bmatrix} \sum_{u\leq k-i-1} \begin{bmatrix} t-i \\ u \end{bmatrix} (-1)^{u}$$

$$= \begin{bmatrix} t \\ i \end{bmatrix} (-1)^{k-i-1} \begin{bmatrix} t-i-1 \\ k-i-1 \end{bmatrix}$$

(The last equality follows by a trivial induction.)

Insert the value for γ_{ti} in (6) yields

$$(7)\qquad (-1)^{k-i-1}\begin{bmatrix} t\\ i\end{bmatrix}\begin{bmatrix} t-i-1\\ k-i-1\end{bmatrix} f_t^{-1}f_i = \prod_{\substack{r<k\\ r\neq i}} \frac{r\pi - t\pi}{r\pi - i\pi}$$

for all $t \geq k$ and all $i < k$.

In particular for $i = 0$ (note $k \geq 2$) and $t \geq k$

$$(-1)^{k-1}\begin{bmatrix} t-1\\ k-1\end{bmatrix} f_t^{-1} = \prod_{0<r<k} \frac{r\pi - t\pi}{r\pi} \quad (\text{note } 0\pi = 0).$$

Insert f_t^{-1} in (7) yields

$$(-1)^{k-i-1}\begin{bmatrix} t\\ i\end{bmatrix}\begin{bmatrix} t-i-1\\ k-i-1\end{bmatrix}(-1)^{k-1}\begin{bmatrix} t-1\\ k-1\end{bmatrix}^{-1}\left[\prod_{0<r<k}\frac{r\pi - t\pi}{r\pi}\right] f_i$$

$$= \prod_{\substack{r<k\\ r\neq i}} \frac{r\pi - t\pi}{r\pi - i\pi}.$$

By easy calculations it follows for $i \neq 0$

$$(-1)^{i}\frac{t}{t-i}\begin{bmatrix} k-1\\ i\end{bmatrix} f_i = \prod_{\substack{r<k\\ r\neq i}} \frac{r\pi - t\pi}{r\pi - i\pi}\ \prod_{0<r<k}\frac{r\pi}{r\pi - t\pi}$$

$$= \left[\prod_{\substack{r<k\\ r\neq 0,i}} \frac{r\pi - t\pi}{r\pi - i\pi}\right]\left[\frac{-t\pi}{-i\pi}\right]\left[\prod_{\substack{r<k\\ r\neq 0,i}}\frac{r\pi}{r\pi - t\pi}\right]\left[\frac{i\pi}{i\pi - t\pi}\right],$$

and therefore

$$(8)\qquad (-1)^{i}\begin{bmatrix} k-1\\ i\end{bmatrix}^{-1} f_i^{-1}\prod_{\substack{r<k\\ r\neq 0,i}}\frac{r\pi}{r\pi - i\pi} = \frac{t}{t-i}\left[\frac{i\pi - t\pi}{t\pi}\right]$$

for all $0 < i < k$ and all $t \geq k$.

Since the left hand side of (8) does not depend on t we obtain

$$(9)\qquad \frac{i\pi - t\pi}{i-t}\cdot\frac{t}{t\pi} = \frac{i\pi - k\pi}{i-k}\cdot\frac{k}{k\pi}$$

for all $i < k$ and all $t \geq k$.

Hence

$$t\pi[i(i\pi)k - i(k\pi)k - t(i\pi)k + ti(k\pi)] = (i\pi)t(i-k)k\pi \neq 0$$
$$\text{for} \quad 0 < i < k \quad \text{and} \quad t \geq k \; .$$

For $i = 1$ (note $k \geq 2$) we get

$$(\underline{10}) \qquad t\pi = \frac{t(1-k)k\pi}{k(1-k\pi) - t(k-k\pi)}$$

for all $t \geq k$ (observe $1\pi = 1$). Insert in ($\underline{9}$) and divide by $t(k\pi) \neq 0$ yields

$$(\underline{11}) \qquad (t-k)i\pi[k(1-k\pi) - i(k-k\pi)] = (t-k)i(k\pi)(1-k) \; .$$

Since $k < p-1$ choose $t > k$ and divide ($\underline{11}$) by $t-k$. Observe that the right hand side of ($\underline{11}$) is different from 0 for $i \neq 0$. Thus

$$(\underline{12}) \qquad i\pi = \frac{i(1-k)k\pi}{k(1-k\pi) - i(k-k\pi)} \quad \text{for} \quad 1 \leq i < k$$

This equation also holds for $i = 0$ as $0\pi = 0$. Together with ($\underline{10}$) it follows

$$(\underline{13}) \qquad i\pi = \frac{i(1-k)k\pi}{k(1-k\pi) - i(k-k\pi)} \quad \text{for} \quad i = 0,1,\ldots,p-1 \; .$$

The denominator of ($\underline{13}$) is different from zero for $0 \leq i \leq p-1$. Now if $k \neq k\pi$ then

$$i = \frac{k(1-k\pi)}{k-k\pi}$$

annihilates this denominator, a contradiction. Thus $k\pi = k$ and then, by ($\underline{13}$), $i = i\pi$ for all i as asserted.

<u>Proposition</u>. Let G be a permutation group of degree p^m where p is an odd prime and $m \geq 2$. Suppose $p \neq 3$ if $m = 2$. If $AGL(m,p) \leq G$ then G is isomorphic to one of the following groups:

$$AGL(m,p) \; , \quad A_{p^m} \quad \text{or} \quad S_{p^m} \; .$$

<u>Proof</u>. First note that G is doubly transitive since the only faithful permutation representation of $AGL(m,p)$ of degree $\leq p^m$ is the natural one on the vector space $V(m,p)$

(see for instance 1.1 of [4]). Let N be a minimal normal subgroup of G. Then by Burnside ([2], Chap. XI, 7.12), N is regular or simple, primitive with $C_G(N) = 1$.

First, suppose that N is regular, hence an elementary abelian p-group of rank m. Furthermore, $G = N \rtimes G_\alpha$ where G_α denotes the stabilizer of a point. $G_\alpha \leq GL(m,p)$ and $AGL(m,p) \leq G$ imply $G = AGL(m,p)$.

Thus we may assume that N is simple, primitive and $C_G(N) = 1$. Write $AGL(m,p) = E \rtimes GL(m,p)$ and note that $G \leq Aut(N)$. As $m \geq 2$ and $p \geq 5$ in case $m = 2$, the affine special linear group $ASL(m,p)$ is perfect.

Thus $ASL(m,p) \subseteq N$, since $Aut(N)/N$ is solvable by Schreier's conjecture.

In particular, N is doubly transitive. Now we can use the list in [1] of simple doubly transitive permutation groups.

As $m \geq 2$, only the following possibilities may occur:

N		degree
A_n	$(n \geq 5)$	n
$PSL(d,q)$	$(d \geq 2)$	$(q^d-1)/(q-1)$
$PSU(3,q^2)$		q^3+1
${}^2B_2(q)$		q^2+1
${}^2G_2(q)$	$(q = 3^u)$	q^3+1
$PSp(2d,2)$	$(d > 2)$	$2^{2d-1} + 2^{d-1}$
$PSp(2d,2)$	$(d > 2)$	$2^{2d-1} - 2^{d-1}$

${}^2G_2(q)$ and $PSp(2d,2)$ do not appear as their degrees are even.

For the Suzuki groups we have $|{}^2B_2(q)| = (q^2+1)q^2(q-1)$ and $p^m = q^2+1$. Since $p \neq 2$, p does not divide $(q-1)$. Comparing the p-parts of $|{}^2B_2(q)|$ and $|ASL(m,p)|$, a contradiction follows. Suppose $N = PSU(3,q^2)$. Then

$$|N| = (q^3+1)q^3(q^2-1)/(3,q+1) \quad \text{and} \quad q^3+1 = p^m .$$

Since $|ASL(m,p)|_p = p^{m+\binom{m}{2}}$, this implies

$$p^{\binom{m}{2}} \;\Big|\; \frac{q^2-1}{(3,\ q+1)} < q^3+1 = p^m , \text{ so } m = 2 .$$

Moreover, $p \mid q^2-1$ and $p \mid q^3+1$, hence $p \mid (q^3+1) + (q^2-1) = q^2(q+1)$, so $p \mid q+1$, in particular $p-1 \leq q$. Hence $(p-1)^3 \leq q^3 = p^2-1 = (p+1)(p-1)$, so $p^2-2p+1 = (p-1)^2 \leq p+1$ and $p(p-3) \leq 0$, i.e. $p \leq 3$, a contradiction again.

Finally, we have to deal with $N = PSL(d,q)$ for $d \geq 2$ and $p^m = \frac{q^d-1}{q-1}$.

If $q = 2$ and $d = 6$ then $\frac{q^6-1}{q-1} = 63 = 3 \cdot 21 \neq p^m$. If $d = 2$ then $|PSL(2,q)| = \frac{(q+1)q(q-1)}{(2,q-1)}$ and $q+1 = p^m$. As $p \neq 2$, p does not divide $q-1$. Then $p^m = |PSL(2,q)|_p < |ASL(m,p)|_p$ yields a contradiction.

Now by a result of Zigmundy ([2], Chap. IX, 8.3)

$$p \mid q^d-1 , \text{ but } p \nmid q^i-1 \text{ for } 0 < i < d .$$

In particular

$$|PSL(d,q)|_p = \left| q^{\binom{d}{2}} \cdot \frac{q^d-1}{q-1} \cdot \frac{(q^{d-1}-1)\cdot\ldots\cdot(q-1)}{(d,\ q-1)} \right|_p$$

$$= \frac{q^d-1}{q-1} = p^m < |ASL(m,p)|_p$$

and the proof is complete.

The case $r = (m-1)$ is trivial.

<u>Proof of the Theorem</u>. Lemma 2 states the assertion for $r = 0$ and $r = m(p-1)-1$. Lemma 4 deals with the case $m = 1$. By ([5], Chap. 13, §9), the Theorem holds if p is even. For $m = 2$ and $p = 3$ the result is contained in Lemma 3.

Thus we may assume that $0 < r < m(p-1)-1$, that $m \geq 2$ and that p is odd (and $p \neq 3$ if $m = 2$). Since

$$AGL(m,p) \leq G = P\,Aut(GRM(r,m)) ,$$

the proposition implies that $G = AGL(m,p)$ or $A_{p^m} \leq G$. In the second case it follows from ([3], Theorem 4.4) that $GRM(r,m)$ is isomorphic to the repetition code, its dual or the whole space (as $p^m \geq 7$), i.e. $r = 0$, $m(p-1)-1$ or $m(p-1)$, a contradiction. Therefore, $G = AGL(m,p)$; by (<u>A</u>) and (<u>B</u>) then

$$Aut(GRM(r,m)) = \mathbb{F}_p^* \times AGL(m,p)$$

as claimed.

References:

[1] P.J. Cameron, "Finite permutation groups and finite simple groups". Bull. London Math. Soc. 13 (1981), 1 - 22.

[2] B. Huppert, N. Blackburn, "Finite groups II, III". Springer, Berlin (1982).

[3] W. Knapp, P. Schmidt, "Codes with prescribed permutation group". J. Alg. 67 (1980), 415 - 435.

[4] R. Knörr, W. Willems, "A characterization of generalized Reed-Muller codes". Submitted J. Comb. Theory.

[5] F.J. MacWilliams, N.J.A. Sloane, "The theory of error correcting codes". North Holland, Amsterdam (1977).

[6] J.H. van Lint, "Coding theory". LNM 201, Springer, Berlin (1973).

Reinhard Knörr
Department of Mathematics
University of Essen
4300 Essen 1
West Germany

Wolfgang Willems
Department of Mathematics
University of Mainz
6500 Mainz
West Germany