MAXIMAL PARTIAL LINE SPREADS OF $PG(3, q)$, q EVEN

Maria Scafati Tallini

Abstract. Applying the representation of $PG(3, q)$ over $AG(2, q)$, [3], we construct a maximal partial line spread of $PG(3, q)$, $q = 2^{2n}$, n an integer, $n \geq 1$, of size $q^2 = q + 2$. This size is the greatest known till now, except a sporadic case, found by O. Heden [2], for $q = 7$.

1. Introduction

Using the representation of $PG(3, q)$ over $AG(2, q)$ explained in [3], we construct a maximal partial line spread of $PG(3, q)$, $q = 2^{2n}$, n an integer, of size $q^2 = q + 2$. A spread of this cardinality has been constructed by J.W. Freeman [1]. This cardinality is the greatest known till now, except a sporadic case for $q = 7$, found by O. Heden [2].

For the notations and theorems about the representation of $PG(3, 2^{2n})$ over $AG(2, 2^n)$, we refer to the paper [3] cited in the bibliography, which the reader must know before reading this text.

Let $GF(q)$ be the Galois field of order q, with $q = 2^{2n}$, n an integer, $n \geq 1$. An element $x \in GF(q)$ is called *cube*, if there is $y \in GF(q)$ such that $x = y^3$. Let $\mathcal{C}$ be the set of cubes of $GF(q)$. The multiplicative group $\mathcal{G}$ of $GF(q)$ is cyclic and then it admits a generator g. It follows that $\mathcal{G} = \{g, g^2, ..., g^{q-1} = 1\}$ and that $|\mathcal{G}| \geq 3$.

Theorem 1. *If g is a generator of $GF(2^{2n})$, then $g \notin \mathcal{C}$.*

Proof. Assume $g \in \mathcal{C}$. There is then $b \in GF(2^{2n})$, such that $g = b^3$. Moreover, $b = g^m$, m and integer and $1 \leq m \leq q - 1$. Therefore, $g = g^{3m}$, whence $3m \equiv 1 \bmod(q - 1)$. By this and by $1 \leq m \leq q - 1$ (which implies $3 \leq 3m \leq 3q - 3$), it follows

(i) $3m = q$,

(ii) $3m = 2q - 1$,

(iii) $3m = 3q - 2$.

The condition (i) is not true, since q is not a multiple of 3, (iii) is also not true, since 2 is not a multiple of 3. Therefore, m must satisfy (ii). We get:

$$q = 2^{2n} = (3-1)^{2n} = (3+(-1))^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} 3^j (-1)^{2n-j}.$$

It follows that q is of the form:

$$q = 3^M + 1,$$

with M an integer. By this and by (ii), it follows:

$$3m = 2(3M+1) - 1 = 6M + 1,$$

a contradiction, since 1 is not a multiple of 3. This contradiction proves that g is not a cube. ∎

From this theorem, we get that $GF(2^{2n}) - \mathcal{C} \neq \emptyset$. Since 1 is a cube, it follows that $\mathcal{C} - \{0\} \neq \emptyset$. Therefore, *in* $GF(2^{2n})$ *there are cubes and not cubes.*

Now, let $m \in \mathcal{C} - \{0\}$, $\overline{m} \in GF(2^{2n}) - \mathcal{C}$. Let $PG(2, 2^{2n})$ be the projective space of dimension 3 over $GF(2^{2n})$ and let $AG(2, 2^{2n})$ be the affine plane over $GF(2^{2n})$. Fix a coordinate system (X, Y) in $AG(2, 2^{2n})$. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be the parabolas of $AG(2, 2^{2n})$ with the equations:

$$\mathcal{P}_1 : y = mx^2,$$
$$\mathcal{P}_2 : \overline{m}x^2.$$

Let $P_1(X_1, Y_1)$ and $P_2(X_2, Y_2)$ be two points of $AG(2, 2^{2n})$, with $P_1 \in \mathcal{P}_1$, $P_2 \in \mathcal{P}_2$, $P_1 \neq P_2$. The line through P_1 parallel to the x axis and the line through P_2 parallel to the y axis meet at the point $A(X_2, Y_1)$. The line through P_1 parallel to the y axis and the line through P_2 parallel to the x axis meet at the point $B(X_1, Y_2)$. Obviously, $A \neq B$. We call the ordered pair (A, B) the *pair associated* with the pair (P_1, P_2). Let (A', B') be the pair associated with (P_1', P_2'), with $(A', B') \neq (A, B)$. We remark that $A \neq A'$, $B \neq B'$. For, if $A = A'$, then $P_1 = P_1'$, $P_2 = P_2'$ and then $B = B'$, whence $(A, B) = (A', B')$, a contradiction. This contradiction proves that $A \neq A'$. Similarly, we prove that $B \neq B'$.

Theorem 2. *The lines* AA' *and* BB' *are not parallel.*

Proof. Let us distinguish the following three cases:

(a) AA' is parallel to the y axis,

(b) BB' is parallel to the y axis,

(c) neither AA', or BB' are parallel to the y axis.

Let us prove (a).

If the line AA' is parallel to the y axis, the lines AP_1 and $A'P_1'$ coincide and then necessarily $P_1 = P_1'$. It follows that the line BB' is parallel to the x axis and then AA' and BB' are not parallel.

Let us prove (b). If the line BB' is parallel to the y axis, then the lines BP_2 and $B'P_2'$ coincide and then necessarily $P_2 = P_2'$. It follows that the line AA' is parallel to the x axis and then AA' and BB' are not parallel.

Let us prove (c). Now, let AA' and BB' be not parallel to the y axis. Let $m(A, A')$ be the slope of the line AA' and $m(B, B')$ the slope of the line BB'.

We get:

$$\begin{aligned} m(A, A') &= \frac{Y_2 - Y_2'}{X_1 - X_1'}, \\ m(B, B') &= \frac{Y_1 - Y_1'}{X_2 - X_2'}, \end{aligned}$$

with $X_1 \neq X_1'$, $X_2 \neq X_2'$.

Then

$$\begin{aligned} &AA' \text{ parallel to } BB' \Longleftrightarrow m(A, A') = m(B, B') \\ &\Longleftrightarrow (Y_2 - Y_2')(X_2 - X_2') = (Y_1 - Y_1')(X_1 - X_1') \\ &\Longleftrightarrow Y_1X_1 - Y_1X_1' - Y_1'X_1 + Y_1'X_1' = Y_2X_2 - Y_2X_2' - Y_2'X_2 + Y_2'X_2'. \end{aligned}$$

Since the characteristic of $GF(2^{2n})$ is two, since $Y_1 = mX_1^2$, $Y_1' = mX_1'^2$ and $Y_2 = \overline{m}X_2^2$, $Y_2' = \overline{m}X_2'^2$, we get:

$$\overline{m} = \frac{m(X_1 + X_1')^3}{(X_2 - X_2')^3}\,.$$

Therefore AA' and BB' are parallel if and only if

$$\overline{m} = \frac{m(X_1 + X_1')^3}{(X_2 - X_2')^3}\,.$$

Then AA' and BB' are not parallel, otherwise $\overline{m}$ is a cube ($m \in \mathcal{C}$), but $\overline{m} \in GF(2^{2n}) - \mathcal{C}$. Therefore the theorem is completely proved. ∎

Remark that the line AB is distinct from the y axis. For, if this line coincides with the y axis, then P_1 and P_2 belonged both to the y axis, a contradiction, otherwise they should coincide with the origin O. The contradiction proves the remark.

Remark also that $A \neq O$, $B \neq O$. For, if $A = O$, then $P_2 = O$, $P_1 = O$, a contradiction, since $P_1 \neq P_2$. Then $A \neq O$ and similarly $B \neq O$.

Theorem 3. *The line AB does not pass through the origin O.*

Proof. If $O \in AB$, since the line AB is distinct from the y axis, it has the equation $y = \alpha x$, $\alpha \in GF(2^{2n})$. Moreover $A \neq O$, $B \neq O$, and then $X_1 \neq O$, $X_2 \neq O$. Then we get:

$$\alpha = \frac{Y_2}{X_1} = \frac{Y_1}{X_2},$$

that is $X_2Y_D = X_1Y_1$.

From this and by $Y = \overline{m}X_2^2$, $Y_1 = mX_1^2$, we get

$$\overline{m}X_2^3 = mX_1^3,$$

whence $\overline{m} \in \mathcal{C}$, a contradiction, since $\overline{m} \notin \mathcal{C}$. The contradiction proves that the line AB does not pass through O, that is Theorem 3. ∎

2. Construction of a maximal partial line spread of $PG(3, 2^{2n})$, n integer, $n \geq 1$

Denote by r_0 the line of $PG(3, 2^{2n})$ belonging to the class b) of [3] represented in $AG_2(2, 2^{2n})$ (see Sections 2 and 3 of [3]) by the proper line pencil with centre O. Let

$$\begin{aligned} \mathcal{S} &= \{(P_1, P_2) : P_1 \in \mathcal{P}_1,\ P_2 \in \mathcal{P}_2,\ P_1 \neq P_2\}, \\ S &= \{(A, B) : (A, B) \text{ is the pair associated with the pair } (P_1, P_2), \\ &\quad \text{with } (P_1, P_2) \in \mathcal{S}\}. \end{aligned}$$

Denote by $\ell(U_1, U_2)$ the line of $PG(3, 2^{2n})$ belonging to the class a) of [3], represented by the ordered pair of distinct points (U_1, U_2) of $AG(2, 2^{2n})$ and let

$$\mathcal{F} = \{v, r_0\} \cup \{\ell(A, B)\}_{(A,B) \in S}.$$

Let us prove the

Theorem 4. *The set of lines $\mathcal{F}$ of $PG(3, 2^{2n})$ is a total spread.*

Proof. We get:

(α) $v \cap r_0 = \emptyset$, since r_0, which is a line of the plane π (see [3]), is represented by a proper pencil of lines of $AG(2, 2^{2n})$ and then does not contain $Y = v \cap \pi$.

(β) $v \cap \ell(A, B) = \emptyset$, $\forall (A, B) \in S$, since the ordered pairs of distinct points of $AG(2, 2^{2n})$ represent the lines of the class a) of [3] of $PG(3, 2^{2n})$ not meeting v and not in π.

(γ) $r_0 \cap \ell(A, B) = \phi$, $\forall (A, B) \in S$, since in Theorem 3 we have proved that the line AB, with $(A, B) \in S$ does not pass through the origin O.

(δ) Two distinct lines $\ell(A, B)$ and $\ell'(A', B')$ with $(A, B) \in S$, $(A', B') \in S$ are not incident, since we proved in Theorem 2 that the lines AA' and BB' are not parallel.

Since the pairs of S, associated with distinct pairs of $\mathcal{S}$ are distinct, it follows

$$|S| = |\mathcal{S}| = q^2 - 1,$$

because the number of pairs of points $(P_1, P_2) \in \mathcal{S}$ except the pair $(0,0)$ is $q^2 - 1$.

By that and since the lines of $PG(2, 2^{2n})$ represented by distinct pairs of S are distinct, it follows that

$$|\{\ell(A,B)\}_{(A,B)\in S}| = q^2 - 1.$$

By the previous arguments and by the definition of $\mathcal{F}$, it follows that

$$|\mathcal{F}| = q^2 + 1.$$

Then $\mathcal{F}$ is a total spread, since it is a covering of $PG(3, 2^{2n})$. ■

Now, let us call *regulus* of $PG(3, 2^{2n})$ a regulus of a hyperbolic quadric of $PG(3, 2^{2n})$. A total spread $\mathcal{F}'$ of $PG(3, 2^{2n})$ is called *regular*, if for any three distinct lines of $\mathcal{F}'$ the regulus containing such lines consists of lines of $\mathcal{F}'$.

Now, let us prove the following

Theorem 5. *Let t_1 and t_2 be two distinct and not parallel lines of $AG(2, 2^{2n})$ and let O be their common point. Let A be a point of $t_1 - \{O\}$ and B a point of $t_2 - \{O\}$. Let r_0 be the line of the plane π (see* [3], Theorem 4 of Section 2, for $r = 3$) *represented in $AG(2, 2^{2n})$ by the pencil with centre O. Let ℓ be the line of $PG(3, 2^{2n})$ represented by the ordered pair of distinct points (A, B) (see* [3], Theorem 3, for $r = 3$)*, the lines v (see* [3]*), r_0 and ℓ being mutually skew. Denote by $\mathcal{I}$ the hyperbolic quadric of $PG(3, 2^{2n})$ determined by v, r_0, ℓ and let $\mathcal{R}$ be the regulus containing such three lines. We prove that the remaining lines of $\mathcal{R}$ are represented in $AG(2, 2^{2n})$ by the ordered pairs of distinct points (A', B'), with $A' \neq O$, $A' \neq A$, $B' \neq O$, $B' \neq B$ and $A'B'$ parallel to AB.*

Proof. (see Figure 1). The line u_1 of $PG(3, 2^{2n})$ represented in $AG(2, 2^{2n})$ in the following way (see [3], Theorem 3, Section 2, for $r = 3$):

$$u_1 : \{(t_1, t), \text{ with } t \text{ a line of } AG(2, 2^{2n}) \text{ parallel to } t_1 \ (t \neq t_1)\}$$

contains U_1, meets r_0 at the point T_1, represented by the line t_1 and meets ℓ at the point of $PG(3, 2^{2n})$, represented in $AG(2, 2^{2n})$ by the ordered pair of distinct lines (t_1, t_1'), where t_1' is the line parallel to t_1 through B. The line u_2 of $PG(3, 2^{2n})$ represented in $AG(2, 2^{2n})$ as follows:

$$u_2 : \{(t, t_2), \text{ with } t \text{ a line of } AG(2, 2^{2n}) \text{ parallel to } t_2 \ (t_1 \neq t_2)\}$$

contains U_2, meets r_0 at the point T_2, represented in $AG(2, 2^{2n})$ by the line t_2 and meets ℓ at the point represented in $PG(2, 2^{2n})$ by the ordered pair (t_2', t_2), where t_2' is the line through A parallel to t_2. The line s of the plane π, represented in $AG(2, 2^{2n})$ by the improper pencil of lines parallel to AB, meets v at Y, r_0 at T, distinct from T_1 and T_2, represented in $AG(2, 2^{2n})$ by the line through O parallel to AB and meets ℓ at the point L, belonging to the plane π, represented by the line AB. Therefore, the lines u_1, u_2 and s belong to the regulus $\mathcal{R}'$ of $\mathcal{I}$, opposite to $\mathcal{R}$. Now, let $A' \in t' - \{O, A\}$ and $B' \in t_2 - \{O, B\}$, such that A', B' is parallel to AB. The line ℓ' of $PG(3, 2^{2n})$, represented by the pair (A', B') meets u_1 at the

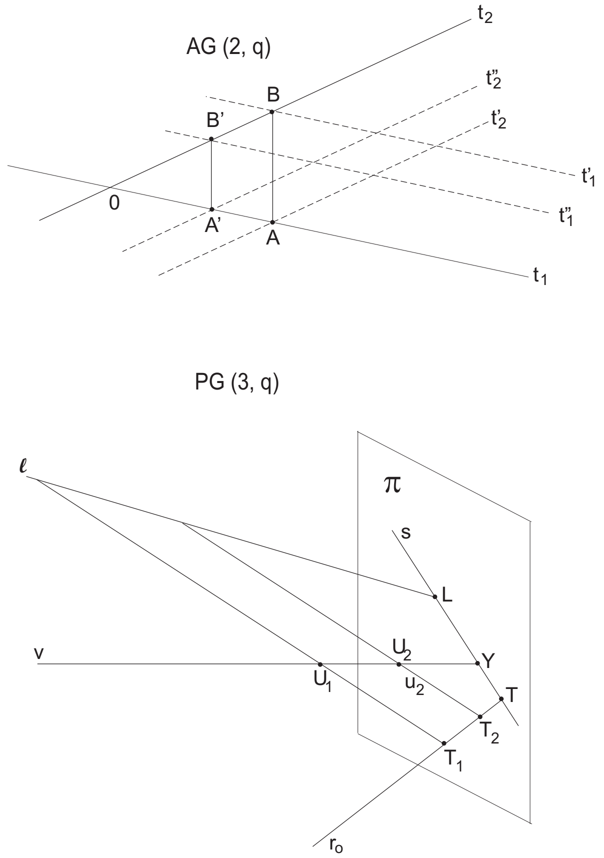

Figure 1

point represented by the ordered pair (t_1, t_1''), where t_1'' is the line through B' parallel to t_1. The line ℓ' meets u_2 at the point represented by the ordered pair (t_2'', t_2), where t_2'' is the line through A' parallel to t_2'. The line ℓ' meets s at the point represented by the line $A'B'$. Therefore the line ℓ' $(\ell' \neq \ell, v, r_0)$ meets u_1, u_2, s. It follows that $\ell' \in \mathcal{R}$. By varying of A' in $t_1 - \{O\}$, we obtain $q-2$ pairs (A', B'), representing the lines of the regulus $\mathcal{R}$, distinct from v, r_0, ℓ. Therefore, we get in the whole $q+1$ lines of $\mathcal{R}$, that is the whole regulus $\mathcal{R}$ which is so represented by the lines v, r_0, ℓ and by the pairs (A', B'), with $A' \in t_1 - \{O, A\}$. ∎

Now, let us prove the following

Theorem 6. *The spread $\mathcal{F}$ is not regular.*

Proof. Let $\overline{P}_2$ be a point of $\mathcal{P}_2 - \{O\}$ and let $(\overline{A}, \overline{B})$ the pair of S associated with the pair $(O, \overline{P}_2)$ of $\mathcal{S}$. Obviously, $\overline{A} \in y$ axis $-\{O\}$, $\overline{B} \in x$ axis $- \{O\}$. Let

$\mathcal{I}$ be the hyperbolic quadric of $PG(3,2^{2n})$ containing the lines v, r_0 and $\ell(\overline{A},\overline{B})$ of $\mathcal{F}$. Let $\mathcal{R}$ be the regulus of $\mathcal{I}$ containing such lines. Let ℓ' be a line of $\mathcal{R}$ distinct from v, r_0 and $\ell(\overline{A},\overline{B})$. Since the line ℓ' does not meet v (since it belongs to the same regulus of v) and does not belong to the plane π, since it does not meet r_0, it belongs to the class a) of [3] and therefore is represented by an ordered pair (A',B') of distinct points of $AG(2,2^{2n})$.

By Theorem 5, we get:

$$A' \in y \text{ axis} - \{O,\overline{A}\},$$
$$B' \in x \text{ axis} - \{O,\overline{B}\},$$
$$A'B' \text{ is parallel to } AB.$$

We remark that $\ell' \notin \mathcal{F}'$. For, ℓ is obviously distinct from v and r_0. Moreover, it is easy to prove that $\ell' \neq \ell(AB)$, for any pair (A,B) associated with a pair (P_1,P_2) of $\mathcal{S}$, with $P_1 \neq O$. It is now to prove that ℓ' is distinct from each of the lines $\ell(AB)$, with (A,B) associated with (O,P_2), $P_2 \in \mathcal{P}_2 - \{O\}$. To do this, let T be the point common to the line through A' parallel to the x axis and to the line through B' parallel to the y axis. The distinct points O, T_2, T are collinear over a line b, as it is easy to prove. If the pair (A',B') is associated with a pair (O,P_2), $P_2 \in \mathcal{P}_2 - \{O\}$, necessarily $T_2 = P_2$ and therefore $T \in \mathcal{P}_2$, a contradiction, since the line b cannot meet $\mathcal{P}_2$ at three distinct points. The contradiction proves that (A',B') is not associated with any pair (O,P_2), $P_2 \in \mathcal{P}_2 - \{O\}$ and then $\ell' \in \mathcal{F}'$. The previous remark is therefore proved. It follows that $\mathcal{R}$ is not entirely consisting of lines of $\mathcal{I}$ and hence it is not regular. ∎

By the above arguments, we get that in $PG(3,2^{2n})$ there is a total non-regular line spread. As such a spread gives rise to an affine non-desarguesian translation plane of order 2^{4n}, we get the following

Theorem 7. *For any $q = 2^{2n}$, n an integer, $n \geq 1$, there exists a non-desarguesian affine plane of order 2^{4n}.*

Let $\mathcal{T}$ be the following set of lines of $PG(3,2^{2n})$:

$$\mathcal{T} = \{\ell(A,B) : (A,B) \text{ is associated with } \{(O,P_2),\ P_2 \in \mathcal{P}_2 - \{O\} \cup \{v, r_0\}.$$

The set $\mathcal{T}$ is a subset of $\mathcal{F}$ and has size $q+1$, but $\mathcal{T}$ is not a regulus of $PG(3,2^{2n})$, since $\mathcal{T}$ contains v, r_0 and $\ell(\overline{A},\overline{B})$ and does not contain $\ell'(A',B')$ (see Theorem 6) which is a line of the regulus $\mathcal{R}$ containing v, r_0 and $\ell(\overline{A},\overline{B})$. Let T_1 and T_2 be the points of $\pi - \{Y\}$ represented by the x axis and the y axis, respectively. The line U_2T_1 of $PG(3,2^{2n})$ meets v at U_2, r_0 at T_1 and $\ell(A,B) \in \mathcal{T} - \{v, r_0\}$ at the point represented by the ordered pair $(t_A, x \text{ axis})$, where t_A is the line of $AG(2,2^{2n})$ through A and parallel to the x axis. It follows that the line U_2T_1 meets all the lines of $\mathcal{T}$. The line U_1T_2 of $PG(3,2^{2n})$ meets v at U_1, r_0 at T_2 and $\ell(A,B) \in \mathcal{T} - \{v, r_0\}$ at the point represented by the ordered pair $(y \text{ axis}, t_B)$, where t_B is the line of $AG(2,2^{2n})$ through B parallel to the y axis. It follows that

U_1T_2 meets all the lines of $\mathcal{T}$. The line U_1T_2 of $PG(3, 2^{2n})$ meets v at U_1, r_0 at T_2 and $\ell(A, B) \in \mathcal{T} - \{v, r_0\}$ at the point represented by the ordered pair (y axis, t_B), where t_B is the line of $AG(2, 2^{2n})$ through B parallel to the y axis. It follows that U_1T_2 meets all the lines of $\mathcal{T}$. The lines U_1T_2 and U_2T_1 are mutually skew (as it is easy to prove by using the representation [3] of $U_1T_2 - \{U_1\}$ and of $U_2T_1 - \{U_2\}$ in $AG(2, 2^{2n})$, or equivalently considering that the lines of $\mathcal{T}$ are mutually skew). Now let

$$\widetilde{\mathcal{F}} = (\mathcal{F} - \mathcal{T}) \cup \{U_1T_2, U_2T_1\}.$$

Obviously, $\widetilde{\mathcal{F}}$ is a line spread of $PG(3, 2^{2n})$. Moreover, $\widetilde{\mathcal{F}}$ is also maximal. For, let ℓ be a line of $PG(3, 2^{2n})$ not meeting any line of $\mathcal{F}$.

Then the points of ℓ range over the $q + 1$ lines of $\mathcal{T}$ and it is $\ell \cap U_1T_2 = \emptyset$, $\ell \cap U_2T_1 = \emptyset$. Then the hyperbolic quadric of $PG(3, 2^{2n})$ containing the three lines U_1T_2, U_2T_1 and ℓ admits $\mathcal{T}$ as one of its reguli. A contradiction, since $\mathcal{T}$ is not a regulus of $PG(3, 2^{2n})$. The contradiction proves that every line of $PG(3, 2^{2n})$ meets some line of $\mathcal{F}$ and then $\mathcal{F}$ is maximal. Moreover

$$|\mathcal{F}| = q^2 - q + 2.$$

Therefore, the following theorem holds:

Theorem 8. *In $PG(3, 2^{2n})$, n integer $n \geq 1$, there is a maximal non-total line spread of size $q^2 - q + 2$.*

This result was obtained by Freeman [1] in 1980, who constructed an example which was the only before this research. Here, we construct a maximal non-total line spread for q even of $PG(3, 2^{2n})$, using only the geometry of the affine plane $AG(2, 2^{2n})$. The cardinality $q^2 - q + 2$ is the maximum known till now, except the sporadic case, for $q = 7$, found by Heden [2].

References

[1] Freeman, J.W., *Reguli and pseudoreguli in $PG(3, 2^{2n})$*, Geom. Dedicata, 9 (1980), 267-280.

[2] Heden, O., *A greedy search for maximal partial spreads in $PG(3, 7)$*, Ars Comb., 32 (1991), 253-255.

[3] Scafati Tallini, M., *Representation of the projective space $P(\tau, k)$ in the affine plane $A(2, k)$*, Proc. Conference on Error-Correcting Codes, Cryptography and Finite Geometries, Amer. Math. Soc. (Eds. A. Bruen and D. Wehlan) (2010), 109-122.

Accepted: 28.06.2012