FINITE SPECIAL MOUFANG SETS OF EVEN CHARACTERISTIC

TOM DE MEDTS[1] YOAV SEGEV[2]

Abstract. We give a short and elementary proof of the fact that a finite special Moufang set with root groups of even order is isomorphic to the unique Moufang set whose little projective group is $\mathrm{PSL}_2(2^k)$ for some integer $k \geq 1$.

Introduction

Moufang sets were introduced in 1990 by J. Tits [T]. Finite Moufang sets had already been studied "avant la lettre" a long time before that as part of the classification of finite split BN-pairs of rank 1. Recall that the class of finite split BN-pairs of rank 1 is a class of doubly transitive groups and that their classification was carried out by Suzuki [Su], Shult [Sh] and Peterfalvi [P1], when the degree is odd and by Hering, Kantor and Seitz [HKSe], when the degree is even. With the exception of Perterfalvi's paper, all these papers are hard and rely, in addition to the Feit-Thompson odd order theorem, on many other deep results in finite group theory.

Our goal in this paper is to give a short and elementary proof for the classification of finite special Moufang sets $\mathbb{M}(U, \tau)$, where $|U|$ is even (i.e. the degree is odd). The paper [S] deals with the case when $|U|$ is odd. Our proof uses the Feit-Thompson Theorem and Glauberman's Z^*-Theorem, but no other deep results are needed. We note that the special Moufang sets form a restricted subclass of all Moufang sets, but nevertheless, our approach illustrates that the new theory of (not necessarily finite) Moufang sets which had been developed so far [DW, DS, SW, DST] can be used to simplify and give more insight into the existing theory of finite Moufang sets.

More precisely, the goal of this paper is to show the following theorem.

Main Theorem. *Let $\mathbb{M}(U, \tau)$ be a finite special Moufang set such that $|U| = q$ is even. Then q is a power of 2, U is elementary abelian and*

Date: January 29, 2007; revised September 18, 2007.

2000 *Mathematics Subject Classification.* Primary: 20E42 ; Secondary: 20B20, 20D05.

Key words and phrases. Moufang set, root group.

[1]Postdoctoral Fellow of the Research Foundation - Flanders (Belgium) (F.W.O.-Vlaanderen).

[2]Partially supported by BSF grant no. 2004-083.

$\mathbb{M}(U,\tau) \cong \mathbb{M}(q)$, the unique Moufang set whose little projective group is $\mathrm{PSL}_2(q)$.

Recall that $\mathbb{M}(U,\tau)$ is special if and only if $(-x)\tau = -(x\tau)$, for all $x \in U^*$. Hence, if U is an elementary abelian 2-group, then $\mathbb{M}(U,\tau)$ is special, and hence we have the following corollary to our Main Theorem.

Corollary. *Let $\mathbb{M}(U,\tau)$ be a finite Moufang set such that U is an elementary abelian 2-group. Then $\mathbb{M}(U,\tau) \cong \mathbb{M}(q)$, the unique Moufang set whose little projective group is $\mathrm{PSL}_2(q)$, where $q = |U|$.*

The crucial point in the proof of the Main Theorem will be to study the two point stabilizer H of the little projective group G, and the proof of the Main Theorem will go in three steps. We first show that $|H|$ is odd and that H acts transitively on the $q-1$ remaining points (i.e. on U^*), then we deduce from this that H is cyclic, and finally we show that this implies that the Moufang set is isomorphic to $\mathbb{M}(q)$.

1. Notation and definitions

We start by fixing the (standard) notation that we will use in this paper.

Notation 1.1 (Notation for groups)**.** Let $\mathcal{G}$ be a group and p a prime.

(1) For $x, y \in \mathcal{G}$, $x^y := y^{-1}xy$ and $[x,y] := x^{-1}y^{-1}xy$.
(2) When we write an inequality sign $\mathcal{H} \leq \mathcal{G}$, we always mean that $\mathcal{H}$ is a *subgroup* of $\mathcal{G}$ (while $\mathcal{A} \subseteq \mathcal{G}$ means that $\mathcal{A}$ is a *subset* of $\mathcal{G}$).
(3) For $\mathcal{A} \subseteq \mathcal{G}$, $\langle \mathcal{A} \rangle$ is the subgroup generated by $\mathcal{A}$.
(4) For a set $\mathcal{A}$ we let $|\mathcal{A}|$ be the cardinality of $\mathcal{A}$.
(5) For an element $g \in \mathcal{G}$, $|g|$ denotes the order of $\mathcal{G}$.
(6) $\mathcal{G}^*$ denotes the set of nontrivial elements of $\mathcal{G}$.
(7) $\mathrm{Inv}(\mathcal{G})$ denotes the set of involutions of $\mathcal{G}$.

Notation 1.2 (Notation for permutation groups)**.** Let $\mathcal{G}$ be a permutation group on a set Ω, and let $Y \subseteq \Omega$ be a nonempty subset.

(1) We let $\mathcal{G}_Y$ be the pointwise stabilizer of Y in $\mathcal{G}$ and we write $\mathcal{G}_{\{Y\}}$ for the global stabilizer of Y in $\mathcal{G}$.
(2) We apply permutations on the right, and for $g \in \mathcal{G}_{\{Y\}}$, $C_Y(g) := \{y \in Y \mid yg = y\}$.

Definition 1.3. A Moufang set $\mathbb{M}$ is a set X together with a collection of groups $U_x \leq \mathrm{Sym}(X)$, one for each $x \in X$, such that each U_x fixes x and acts sharply transitively on $X \setminus \{x\}$, and such that each U_y permutes the set $\{U_x \mid x \in X\}$ by conjugation. The groups U_x are called the root groups of $\mathbb{M}$.

Notation 1.4 (Notation for Moufang sets)**.** Our notation for Moufang sets follows [DS], and we refer the reader to that paper for details. We will briefly recall the construction $\mathbb{M}(U,\tau)$ starting with a group $(U,+)$ and a permutation $\tau \in \mathrm{Sym}(U^*)$.

So let $(U,+)$ be an arbitrary group (possibly non-abelian), and let τ be a permutation of $U^* := U \setminus \{0\}$. We set $X := U \cup \{\infty\}$, and we extend τ to X by $0\tau = \infty$ and $\infty\tau = 0$. For each $a \in U$, we define $\alpha_a \in \mathrm{Sym}(X)$ by $\infty\alpha_a = \infty$ and $x\alpha_a = x + a$ for all $x \in U$. Clearly, $U_\infty := \{\alpha_a \mid a \in U\}$ is a subgroup of $\mathrm{Sym}(X)$ isomorphic to U. We now define $U_0 := U_\infty^\tau$ (by conjugation in $\mathrm{Sym}(X)$), and for each $a \in U^*$ we let $U_a := U_0^{\alpha_a}$. We then write $\mathbb{M}(U,\tau)$ for the collection $(X,(U_x)_{x\in X})$; this is not always a Moufang set, but every Moufang set can be obtained in this way.

Now let $\mathbb{M} := \mathbb{M}(U,\tau)$ be a Moufang set. Throughout this paper we fix the following notation.

(1) G denotes the little projective group $\langle U_x \mid x \in X\rangle$ of $\mathbb{M}$.
(2) $N := G_{\{0,\infty\}}$ is the global stabilizer in G of $\{0,\infty\}$.
(3) $H := G_{0,\infty}$ is the pointwise stabilizer in G of $0,\infty$; this is the *Hua subgroup* of $\mathbb{M}$. Since $\mathbb{M}$ is a Moufang set, H is a subgroup of $\mathrm{Aut}(U)$.
(4) For each $a \in U^*$, we let μ_a be the unique element of the double coset $U_0\alpha_a U_0$ interchanging 0 and ∞.
(5) For a field $\mathbb{F}$, we let $\mathbb{M}(\mathbb{F})$ be the unique Moufang set whose little projective group is isomorphic to $\mathrm{PSL}_2(\mathbb{F})$. More precisely, this is the Moufang set $\mathbb{M}(\mathbb{F}; x \mapsto -x^{-1})$ see [DW, Example 3.1]; we write $\mathbb{M}(q) := \mathbb{M}(\mathbb{F}_q)$.

Definition 1.5. A Moufang set $\mathbb{M} = \mathbb{M}(U,\tau)$ is called special, if we have $(-a)\tau = -(a\tau)$ for all $a \in U^*$.

From now until the end of the paper we assume that $\mathbb{M}(U,\tau)$ is a finite special Moufang set such that $|U|$ is even.

2. H has odd order

Since $|U|$ is even, [DST, Theorem 5.5] implies that U is an elementary abelian 2-group, and by [DS, Lemma 4.3(5)] or [DST, Theorem 6.3], $\mu_x^2 = 1$ for all $x \in U^*$.

Proposition 2.1. (1) *$|H|$ is odd;*
(2) *H is transitive on U^*.*

Proof. The idea of the proof is taken from [P1]. Let

$$\mathcal{I} := \bigcup_{x\in X} U_x^*.$$

Notice that $\mathcal{I} \subseteq \mathrm{Inv}(G)$, and that

$$\text{if } t \in \mathcal{I} \cap G_\infty \text{ then } t \in U_\infty. \tag{2.1}$$

Note further that

$$\text{if } t \in U_\infty^*,\ s \in \mathcal{I}, \text{ and } [s,t]=1, \text{ then } s, st \in U_\infty. \tag{2.2}$$

This is because ∞ is the unique fixed point of t and hence $s \in \mathcal{I} \cap G_\infty$, so by (2.1), $s \in U_\infty$, and then $st \in U_\infty$. It follows that

$$\text{if } s,t \in \mathcal{I} \text{ and } s \notin U_\infty \ni t, \text{ then } |st| \text{ is odd.} \tag{2.3}$$

Indeed, suppose $|st|$ is even, and let $w \in \mathrm{Inv}(\langle st \rangle)$. Then wt is conjugate to t or s (in $\langle s,t \rangle$), so $wt \in \mathcal{I}$ and hence by (2.2), $w \in U_\infty$. Similarly $ws \in \mathcal{I}$, and applying (2.2) once more we see that $s \in U_\infty$, a contradiction.

By (2.3) any involution in U_∞ is conjugate to s and so all involutions in U_∞ are conjugate, that is

$$\mathcal{I} \text{ is a conjugacy class of involutions in } G. \tag{2.4}$$

Note that since any $s,t \in U_\infty^*$ are conjugate in G, they are actually conjugate in $G_\infty = U_\infty H$, so they are conjugate by an element of H; since $\alpha_a^h = \alpha_{ah}$ for all $a \in U$ and $h \in H$, this shows (2).

Further, since $\mu_a^h = \mu_{ah}$ for each $a \in U^*$ and $h \in H$ (see [DS, Prop. 3.9(2)]), it follows that

$$\{\mu_a \mid a \in U^*\} \text{ is a conjugacy class of involutions in } N. \tag{2.5}$$

Notice however that for $a, b \in U^*$ with $a \neq b$, $[\mu_a, \mu_b] \neq 1$, because $\mu_a^{\mu_b} = \mu_{a\mu_b}$ (again by [DS, Prop. 3.9(2)]), so if $\mu_{a\mu_b} = \mu_a$, then by [DS, Prop. 4.9(4)], $a\mu_b = a$; but by [DS, Lemma 4.3(5)], μ_b is conjugate to α_b and therefore has a unique fixed point, which is equal to b by [DS, Lemma 4.3(2)], implying $a = b$.

By (2.5) and Glauberman's Z^*-Theorem (see, e.g., [A, p. 261]), $\mu_a\mu_b \in O_{2'}(N)$, for all $a, b \in U^*$, where $O_{2'}(N)$ is the largest normal subgroup of odd order of N. However by [DW, Theorem 3.1(ii)], $H = \langle \mu_a\mu_b \mid a, b \in U^* \rangle$, so $H \leq O_{2'}(N)$ and hence $|H|$ is odd. □

3. H is cyclic

To show that H is cyclic, we will rely on the following result, the elementary proof of which is due to T. Peterfalvi.

Lemma 3.1. *Let p be an odd prime, let q be an arbitrary prime, and suppose that P is a p-group acting faithfully on an elementary abelian q-group E. If $|C_P(a)| = |C_P(b)|$ for all $a, b \in E^*$, then P is cyclic and $C_E(P) = 0$.*

Proof. See [P2, Lemme, Appendix X, p. 281]. □

Proposition 3.2. *H is cyclic.*

Proof. Recall that $H \leq \mathrm{Aut}(U)$. By Proposition 2.1(1), $|H|$ is odd, so in particular, by the Feit-Thompson theorem H is solvable. By Proposition 2.1(2),

$$|C_{O_p(H)}(e)| = |C_{O_p(H)}(f)|, \quad \text{for all primes } p \text{ and all } e, f \in U^*. \tag{3.1}$$

By (3.1) and Lemma 3.1 (with $O_p(H)$ in place of P and U in place of E), $O_p(H)$ is cyclic, for all odd primes p and hence

(3.2) H is solvable of odd order and the Fitting group $F(H)$ is cyclic.

Now by Proposition 2.1(2), H acts transitively on U^*. Since $F(H)$ is cyclic, every subgroup of $F(H)$ is normal in H, and in particular $\langle h \rangle$ is normal in H for all $h \in F(H)$. Hence

$$C_U(h) = 0, \text{ for all } h \in F(H)^*. \tag{3.3}$$

Let $x \in U^*$ and $h \in F(H)$. If $\mu_{xh} = \mu_x^h = \mu_x$, then $xh = x$ and hence by (3.3), $h = 1$. Hence

$$C_{F(H)}(\mu_x) = 1 \text{ for all } x \in U^*. \tag{3.4}$$

But now, since $\mu_x^2 = 1$, (3.2) and (3.4) imply that μ_x inverts $F(H)$. We thus see that

$$\mu_x \mu_y \in C_H(F(H)) \leq F(H),$$

for all $x, y \in U^*$, so since $H = \langle \mu_x \mu_y \mid x, y \in U^* \rangle$ by [DW, Theorem 3.1(ii)], we see that $H = F(H)$ is cyclic. □

4. Proof of the Main Theorem

We will follow the convention of [DW, Remark 3.2] and choose an identity element $e \in U^*$, so that its Hua map h_e is the identity map on U. We will explicitly reconstruct the field $\mathbb{F}_q$ (with identity e) and show that $\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$.

Proposition 4.1. *$\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$, where $q = |U|$ is a power of 2.*

Proof. Observe that by [DS, Prop. 5.2(4)], we have $h_{ah_b} = h_a h_b^2$ for all $a, b \in U^*$, and since $H = \langle h_a \mid a \in U^* \rangle$, it follows that

$$h_{ah} = h_a h^2 \tag{4.1}$$

for all $a \in U^*$ and all $h \in H$.

Now let $a, b \in U^*$ be arbitrary, and let $h \in H$ be such that $h^2 = h_b$. Then $h_a h_b = h_a h^2 = h_{ah}$ by equation (4.1), and hence $H = \{h_a \mid a \in U^*\}$. Since $h_a = h_b$ if and only if $a = b$ by [DS, Prop. 5.2(5)], this implies that $|H| = |U^*| = q - 1$. In particular, $h^q = h$ for all $h \in H$.

We now define a multiplication on U by setting

$$a \cdot b := a h_b^{q/2}$$

for all $a, b \in U$ (where, by convention, h_0 is the zero map). Then, by equation (4.1), we have $h_{a \cdot b} = h_a h_b^q = h_a h_b$ for all $a, b \in U^*$. Since H is abelian, this implies $h_{a \cdot b} = h_{b \cdot a}$, and hence this multiplication is commutative. It is also associative, since $h_{(a \cdot b) \cdot c} = h_a h_b h_c = h_{a \cdot (b \cdot c)}$ for all $a, b, c \in U^*$. Moreover, it is obvious that $(a + b) \cdot c = a \cdot c + b \cdot c$, so the distributive laws hold. Finally, by construction e is the identity of our multiplication, and this choice forces $\tau = \mu_e$, so $h_a h_{a\tau} = h_e$, for all $a \in U^*$; see for example [DS, Prop. 5.2(3)].

Hence $a \cdot a\tau = e$ for all $a \in U^*$. We conclude that $(U, +, \cdot)$ is a commutative field with identity e and multiplicative inverse τ. Since $|U| = q$, we conclude that this field must be $\mathbb{F}_q$, and hence $\mathbb{M}(U, \tau) \cong \mathbb{M}(q)$; see, for example, [DW, Example 3.1]. □

References

[A] M. Aschbacher, *Finite Group Theory*, Cambridge U. Press, Cambridge, 1986.

[DS] T. De Medts and Y. Segev, "Identities in Moufang sets", to appear in *Trans. Amer. Math. Soc.*

[DST] T. De Medts, Y. Segev and K. Tent, "Some special Features of special Moufang sets", submitted.

[HKSe] C. Hering, W. M. Kantor and G. M. Seitz, "Finite groups with a split BN-pair of rank 1, I", *J. Algebra* **20** (1972), 435–475.

[DW] T. De Medts and R. M. Weiss, "Moufang sets and Jordan division algebras", *Math. Ann.* **335** (2006), no. 2, 415–433.

[P1] T. Peterfalvi, "Sur les BN-paires scindées de rang 1, de degré impair", *Comm. Algebra* **18** (1990), no. 7, 2281–2292.

[P2] T. Peterfalvi, "Le théoréme de Bender-Suzuki II", in *Révision dans les groupes finis. Groupes du type de Lie de rang* 1*, Astérisque* no. **143** (1986), 235–295.

[S] Y. Segev, *Finite special Moufang sets of odd characteristic,* preprint, 2006.

[SW] Y. Segev and R. M. Weiss, "On the action of the Hua subgroups in special Moufang sets", to appear in *Math. Proc. Cambridge Philos. Soc.*

[Sh] E. Shult, "On a class of doubly transitive groups", *Illinois J. Math.* **16** (1972), 434–445.

[Su] M. Suzuki, *On a class of doubly transitive groups II,* Ann. of Math. (2) **79** (1964) 514–589.

[T] J. Tits, "Twin buildings and groups of Kac-Moody type", in *Groups, combinatorics & geometry (Durham, 1990)*, 249–286, London Math. Soc. Lecture Note Ser. **165**, Cambridge Univ. Press, Cambridge, 1992.

Tom De Medts, Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281 S22, 9000 Gent, Belgium
E-mail address: tdemedts@cage.ugent.be

Yoav Segev, Department of Mathematics, Ben-Gurion University, Beer-Sheva 84105, Israel
E-mail address: yoavs@math.bgu.ac.il