QUADRATIC FUNCTIONS AND $GF(q)$-GROUPS

CHRISTOPHER PARKER AND PETER ROWLEY

(Communicated by Ronald M. Solomon)

Abstract. Properties of $GF(q)$-groups are reformulated in terms of quadratic functions and pre-semifields. As a consequence, counter-examples to some earlier results are obtained.

1. Introduction

In this paper we investigate a particular kind of special 2-group. These groups, called groups of $GF(q)$-type, were first defined in [6].

Definition 1.1. Suppose that $q = 2^m$. We say that a group $P$ is of $GF(q)$-type if $P$ is a special 2-group with $|Z(P)| = q$ and if, for every $x \in P \setminus Z(P)$, the following conditions hold:

(i) $[P : C_P(x)] = [Z(C_P(x)) : Z(P)] = q$; and

(ii) for all $y \in Z(C_P(x)) \setminus Z(P)$, $C_P(x) = C_P(y)$.

The primary reason for this article is that we have discovered counter-examples to various of the early lemmas in Timmesfeld’s paper [6]. Since Stroth in [4] employed the same argument as in [6], we also present counter-examples to [4, Main Theorem and Corollary 2]. The root of the problems lies in the proofs of [6, Lemma 1.2] and [4, Lemma 1.1], where the identification with the projective line is not justified. In addition to describing these counter-examples in Theorems 1.5 and 1.6 we consider what can be recovered from [4] and [6].

The most important application of the results proven in [4] and [6] is in the classification of finite simple groups of characteristic 2-type. More precisely, the Main Theorem in [6] must be used whenever Stroth’s Theorem [5] is. It is therefore important to note that Timmesfeld, in a private communication [7], has provided a proof of the Main Theorem of [6] (in a slightly modified form).

Our approach to the problem, as in [4], is via quadratic functions, which are defined as follows:

Definition 1.2. Let $V$ be a vector space over $GF(2)$ and set $q = 2^m$. A surjective function

$$Q : V \rightarrow GF(q)^+$$

is called a quadratic function if the function

$$b : V \times V \rightarrow GF(q)^+;$$

$$(v, w) \mapsto Q(v + w) + Q(v) + Q(w)$$
is $GF(2)$-bilinear. If, in addition, $V$ is a vector space over $GF(q)$, $b$ is $GF(q)$-bilinear and $Q(\lambda v + \mu w) = \lambda^2 Q(v) + \mu^2 Q(w) + \lambda \mu b(v, w)$ for all $\lambda, \mu \in GF(q)$ and $v, w \in V$, then $Q$ is said to be a quadratic form over $GF(q)$.

Suppose that $V$ is a vector space over $GF(2)$, $W$ is a subspace of $V$ and $b : V \times V \to GF(q)^+$ is a symmetric and $GF(2)$-bilinear function. Then we define

$W^\perp = \{ v \in V \mid b(v, w) = 0 \text{ for all } w \in W \}$;

$Q(W) = \{ w \in W \mid Q(w) = 0 \}$; and

$W^\# = W \setminus \{0\}$.

Next we introduce the following hypothesis:

**Hypothesis 1.3.** $V$ is a finite dimensional vector space over $GF(2)$, $q = 2^m$, $Q : V \to GF(q)^+$ is a quadratic function, $\mathcal{U} \subseteq V^\#$ and the following conditions are satisfied:

(i) $V^\perp = 0$;
(ii) for all $v \in \mathcal{U}$, $\dim_{GF(2)} V/v^\perp = \dim_{GF(2)} v^{\perp\perp} = m$;
(iii) for $v \in \mathcal{U}$ and $w \in v^{\perp\perp}$, $w^\perp = v^\perp$; and
(iv) if $v \in \mathcal{U}$ and $Q(v) = 0$, then $Q(w) = 0$ for all $w \in v^{\perp\perp}$.

We will be mainly concerned with the more restrictive situation described in

**Hypothesis 1.4.** Hypothesis 1.3 holds with $\mathcal{U} = V^\#$.

**Theorem 1.5.** Suppose that Hypothesis 1.4 is satisfied with $Q(V) \neq \emptyset$. Then $V = \bigperp_i V_i$ is an orthogonal sum of $2m$-dimensional spaces each satisfying Hypothesis 1.4. Moreover, either each orthogonal summand satisfies $Q(V_i) \neq \emptyset$ or there is a unique $2m$-dimensional orthogonal summand, $R$, for which $Q(R) = \emptyset$.

Notice that the statement in Theorem 1.5 resembles that in [4, Theorem] though in [4] the hypothesis is weaker in that there Hypothesis 1.3 is satisfied with $\mathcal{U} = Q(V)$. At the end of Section 2 we show that there are an infinite number of counter-examples to this stronger statement.

As in [6], we use $D(q)$ to denote a group isomorphic to a Sylow 2-subgroup of $SL_3(q)$.

**Theorem 1.6.** Suppose that $P$ is a $GF(q)$-type group and that if $x$ in $P \setminus Z(P)$ is an involution, then $Z(C_P(x))$ is elementary abelian. If there are involutions in $P \setminus Z(P)$, then $P$ is a central product of $GF(q)$-type groups of order $q^3$. Moreover, either each of the groups of order $q^3$ is isomorphic to $D(q)$ or all but one of the groups is isomorphic to $D(q)$ and the remaining group is isomorphic to a Sylow 2-subgroup of $SU_3(q)$.

Again Theorem 1.6 should be compared with [4, Corollary 2], and the corresponding counter-examples are presented in Section 3.

Theorems 1.5 and 1.6 are proven in Section 4. The counter-examples mentioned above are constructed from semifields and the connection between quadratic functions and semifields is established in Section 2. The relationship between quadratic functions and $GF(q)$-type groups is revealed in Section 3.
2. QUADRATIC FUNCTIONS AND PRE-SEMIFIELDS

The following definition is taken from Dembowski [2, page 237].

**Definition 2.1.** A **pre-semifield** is a set $S$ which has both an addition $+$ and a multiplication $\circ$ and satisfies:

(i) $(S, +)$ is a group (with identity $0$).
(ii) $x \circ (y + z) = x \circ y + x \circ z$.
(iii) $(x + y) \circ z = x \circ z + y \circ z$.
(iv) If $x \circ y = 0$, then $x = 0$ or $y = 0$.

If additionally, there exists $1 \in S$ such that $1 \circ x = x \circ 1 = x$ for all $x \in S$, then we say that $S$ is a **semifield**.

The following observations are extracted from [2, pages 237-238]

**Proposition 2.2.** Suppose that $S$ is a finite pre-semifield. Then

(i) $S$ is a vector space over $GF(p)$ for some prime $p$, the characteristic of the pre-semifield.
(ii) If $\sigma \in S^\#$ and we define a further multiplication $\circ_\sigma$ on $S$ by $(x \circ_\sigma \circ_\sigma)(y) = x \circ y$, then with this new multiplication $S$ becomes a semifield with multiplicative identity $\sigma \circ \sigma$.
(iii) If $S$ is a semifield and $(S \setminus \{0\}, \circ)$ is associative, then $S$ is a field.

Suppose that $Q$ is a quadratic function on a vector space $V$ over $GF(2)$ with associated bilinear map $b$. Note that $b(v, w) = b(w, v)$ and that $Q(0) = 0$. Also, for $v \in V$, $b(v, v) = 0$ implies $v \in v^\perp$ and hence $v^\perp \perp \subset v^\perp$.

**Proposition 2.3.** Suppose that $S$ is a pre-semifield of characteristic 2 and order $q = 2^m$. Then

$$Q : S \times S \to S(\cong GF(q)^+),$$

$$(v, w) \mapsto v \circ w$$

is a quadratic function. Furthermore,

(i) $Q(S \times S) = \{(0, 0), (v, w) \mid v, w \in S\}$;
(ii) $(v, 0)^\perp = (0, 0)^\perp = \{(w, 0) \mid w \in S\}$ for each $v \in S^\#$; and
(iii) $(0, v)^\perp = (0, 0)^\perp = \{(0, w) \mid w \in S\}$ for each $v \in S^\#$.

**Proof.** We need to show that for $v, w, z \in S \times S$

(1) \[ b(v + w, z) = b(v, z) + b(w, z), \]
(2) \[ b(v, w + z) = b(v, w) + b(v, z). \]

Since $b(x, y) = b(y, x)$, it suffices to show that (1) holds.

Let $v = (v_1, v_2), w = (w_1, w_2), z = (z_1, z_2) \in S \times S$. We will employ Definition 2.1 (ii) and (iii) to show that (1) holds. We have

\[ b(v + w, z) = Q(v + w + z) + Q(v + w) + Q(z) = (v_1 + w_1 + z_1) \circ (v_2 + w_2 + z_2) + (v_1 + w_1) \circ (v_2 + w_2) + z_1 \circ z_2 = v_1 \circ v_2 + v_1 \circ w_2 + v_1 \circ z_2 + w_1 \circ v_2 + w_1 \circ w_2 + w_1 \circ z_2 + z_1 \circ v_2 + z_1 \circ w_2 + z_1 \circ z_2 = v_1 \circ z_2 + z_1 \circ v_2 + z_1 \circ w_2 + w_1 \circ z_2. \]
while, on the other hand, we have
\[
b(v, z) + b(w, z) = Q(v + z) + Q(w + z) + Q(v) + Q(w) + Q(z) + Q(z)
\]
\[
= Q(v + z) + Q(w + z) + Q(v) + Q(w)
\]
\[
= (v_1 + z_1) \circ (v_2 + z_2) + (w_1 + z_1) \circ (w_2 + z_2) + v_1 \circ v_2 + w_1 \circ w_2
\]
\[
= v_1 \circ v_2 + v_1 \circ z_2 + z_1 \circ v_2 + z_1 \circ z_2 + w_1 \circ w_2 + w_1 \circ z_2 + z_1 \circ w_2
\]
\[
+ z_1 \circ z_2 + v_1 \circ v_2 + w_1 \circ w_2
\]
\[
= v_1 \circ z_2 + z_1 \circ v_2 + z_1 \circ w_2 + v_1 \circ w_2.
\]
(4)

Thus, as (3) equals (4), (1) holds.

Next for \( v = (v_1, v_2) \in S \times S \) we have \( Q(v) = 0 \) if and only if \( v_1 \circ v_2 = 0 \) which, by Definition 2.1 (iv), is if and only if either \( v_1 = 0 \) or \( v_2 = 0 \). Therefore, \( Q(S \times S) = \{(v, 0), (0, w) | v, w \in S \} \) and (i) holds. Suppose that \( (w_1, w_2) \in S \times S \) and \( b((v, 0), (w_1, w_2)) = 0 \). Then \( 0 = Q((v + w_1, w_2)) + Q((v, 0)) + Q((w_1, w_2)) = (v + w_1) \circ w_2 + 0 \circ 0 = v \circ w_2 \). Hence, by choosing \( v \neq 0 \) we force \( w_2 = 0 \) and so \((v, 0)^\perp = (v, 0) = \{(w, 0) | w \in S \} \). This proves (ii), and (iii) follows by a similar argument.

**Notation.** Suppose that \( S \) is a finite pre-semifield of characteristic 2, and let \( \sigma \in S^\# \) be fixed. Then as \( S \) is a pre-semifield the left and right distributive laws imply that, for \( v, w \in S \), there is a unique solution to each of the equations \( v = v_1 \circ \sigma \) and \( w = \sigma \circ w_1 \). We define \( v \circ_\sigma w = v_1 \circ w_1 \). With this new multiplication \( \sigma \) is a semifield which we denote by \( S_\sigma \). Using Proposition 2.3 we can construct a quadratic function from \( S_\sigma \times S_\sigma \to S_\sigma \). We denote this quadratic function by \( Q_\sigma \), the associated bilinear function by \( b_\sigma \) and the “perps” by \( \perp_\sigma \).

**Proposition 2.4.** Suppose that \( K = GF(q)^+, q = 2^m \), \( V = K \times K \) and \( Q : V \to K \) is a quadratic function which satisfies for every \( h \in K^\# \),

(i) \( Q(h, 0) = Q((0, h)) = 0 \); and

(ii) \( (h, 0)^\perp = \{(l, 0) | l \in K \} \) and \( (0, h)^\perp = \{(0, l) | l \in K \} \).

For \( x, y \in K \) define \( x \circ y = Q((x, y)) \). Then \( (K, +, \circ) \) is a pre-semifield. Furthermore, if \( V \) and \( Q \) satisfy Hypothesis 1.4 and \( K \in K^\# \) is fixed, then \( K_k \cong GF(q) \) is a field and the quadratic function \( Q_k \) is a quadratic form.

**Proof.** We demonstrate that (i)–(iv) of Definition 2.1 hold. Plainly \( K \) is an abelian group under addition. Let \( x, y, z \in K \). Then

\[
x \circ (y + z) = Q((x, y + z)) = Q((x + 0, y + z)) = Q((x, y) + (0, z))
\]
\[
= b((x, y), (0, z)) + Q((x, y)) + Q((0, z))
\]
\[
= b((x, 0), (0, y), (0, z)) + Q((x, y)) + 0
\]
\[
= b((x, 0), (0, z)) + b((0, y), (0, z)) + Q((x, y))
\]
\[
= Q((x, 0) + (0, z)) + Q((x, 0)) + Q((0, z)) + Q((x, y))
\]
\[
= Q((x, z)) + 0 + 0 + Q((x, y))
\]
\[
= Q((x, z)) + Q((x, y)) = x \circ y + x \circ z.
\]

This demonstrates Definition 2.1(ii), and (iii) follows from a similar calculation.

Now we show that part (iv) holds. So by way of a contradiction suppose that \( x, y \in K^\# \) and \( x \circ y = 0 \). Then \( 0 = Q((x, y)) = Q((x, 0) + (0, y)) = b((x, 0), (0, y)) + Q((0, y)) + Q((0, y)) = b((x, 0), (0, y)). \) Hence, as \( (x, 0)^\perp = \{(l, 0) | l \in K \} \) and
(0, y)⊥ = {(0, l) | l ∈ K} we conclude that (x, 0) ∈ {(0, l) | l ∈ K} and (0, y) ∈ {(l, 0) | l ∈ K}, which is a contradiction. Thus Definition 2.1 (iv) is also satisfied and (K, +, ◦) is a pre-semifield.

We now fix k ∈ K# and consider Kk.

(2.4.1) (V, Qk) satisfies Hypothesis 1.4 if and only if (V, Q) satisfies Hypothesis 1.4.

We employ the following notation: if v ∈ K, then v′ is the unique element of K with v = v′ ◦ k and v′′ is the unique element of K which satisfies v = k ◦ v′′.

Since Qk((v, w)) = v ◦ k w = v′ ◦ w′′ = Q((v′, w′′)) it suffices to show that (w1, w2) ∈ (v1, v2)⊥k if and only if (w′1, w′2) ∈ (v′1, v′2)⊥. If v = (v1, v2) and w = (w1, w2), we further observe that b(v, w) = Q(v+w)+Q(v)+Q(w) = v ◦ k w + w ◦ k v and b_k(v, w) = v′ ◦ w′′ + v′ ◦ w′′.

Suppose that (w1, w2) ∈ (v1, v2)⊥. Then

\[ 0 = b_k((w1, w2), (v1, v2)) = w1 ◦ v′′ + v′ ◦ w′′ = b((w′1, w′2), (v′1, v′2)), \]

whence (w′1, w′2) ∈ (v′1, v′2)⊥ and conversely, as required.

We now prove that Kk is a field. It suffices to show that the multiplication (K, ◦k) is associative. We denote by 1_k the identity element of Kk. Then we consider (1_k, 1_k) ∈ V. We get (1_k, 1_k)⊥ = \{(s, s) | s ∈ Kk\}, and so, by dimensions, (1_k, 1_k)⊥k = (1_k, 1_k)⊥k⊥k. Now let (s, s), (t, t) ∈ (1_k, 1_k)⊥k = (1_k, 1_k)⊥k⊥k. Then, by Hypothesis 1.3 (iii), (s, s) ∈ (t, t)⊥k which is to say 0 = b_k((t, t), (s, s)) = t ◦ k s + s ◦ k t. Hence (K, ◦k) is commutative. Next for any non-zero x ∈ K we have (1_k, x)⊥k = \{(s, s ◦ k x) | s ∈ K\}. Suppose that x, s, t are arbitrary elements of K# k. Then, by Hypothesis 1.3 (iii), (s, s ◦ k x) ∈ (t, t ◦ k x)⊥k. Therefore

\[ 0 = b_k((t, t ◦ k x), (s, s ◦ k x)) = t ◦ k (s ◦ k x) + s ◦ k (t ◦ k x) \]

and now using the commutativity of (K, ◦k) twice we get 0 = t ◦ k (x ◦ k s) + (t ◦ k x) ◦ k s. Hence (K, ◦k) is associative and so Kk is a field. As, up to isomorphism, there is a unique field of order 2m we conclude that Kk ≅ GF(q). It now follows immediately that V is a 2-dimensional vector space over Kk.

Finally suppose that μ, λ ∈ Kk and v = (v1, v2), w = (w1, w2) ∈ V. We use the commutativity and associativity of (K, ◦k) in the following calculation.

\[ Q_k(λ ◦ k v + μ ◦ k w) = b_k(λ ◦ k (v1, v2), μ ◦ k (w1, w2)) + Q_k(λ ◦ k (v1, v2)) \]

\[ + Q_k(μ ◦ k (w1, w2)) = b_k((λ ◦ k v1, λ ◦ k v2), (μ ◦ k w1, μ ◦ k w2)) + Q_k((λ ◦ k v1, λ ◦ k v2)) \]

\[ + Q_k((μ ◦ k w1, μ ◦ k w2)) = λ ◦ k v1 ◦ k μ ◦ k w2 + μ ◦ k w1 ◦ k λ ◦ k v2 + λ ◦ k v1 ◦ k λ ◦ k v2 \]

\[ + μ ◦ k w1 ◦ k μ ◦ k w2 = λ ◦ k μ ◦ k v1 ◦ k w2 + μ ◦ k λ ◦ k v1 ◦ k v2 + λ ◦ k λ ◦ k v1 ◦ k v2 \]

\[ + μ ◦ k μ ◦ k w1 ◦ k w2 = (λ ◦ k) ◦ k b_k(v, w) + λ^2 ◦ k Q_k(v) + μ^2 ◦ k Q_k(w). \]

Hence Qk is a quadratic form on V with respect to Kk.

We are now able produce counter-examples to [4, Theorem]. Indeed, assuming that [4, Theorem] is true, we show that every finite semifield is a field. This is
well-known not to be the case – see [2, page 237-245] for infinitely many examples of non-associative semifields.

So suppose that [4, Theorem] is true and assume that \( S \) is any semifield of characteristic 2 and order \( q \). Then, from Proposition 2.3, we may construct a quadratic function,

\[
Q_{S} : S \times S \to S \cong GF(q^{+})
\]
defined by \( Q_{S}(x, y) = x \circ y \). Furthermore, by Proposition 2.3 (i), (ii) and (iii), \( S \times S \) and \( Q_{S} \) satisfy Hypothesis 1.3 with \( U = Q(S \times S) \). Thus [4, Theorem] applies with \( n = 1 \). Therefore, \( Q_{S} \) is a quadratic form. Hence \( S \times S \) and \( Q_{S} \) satisfy Hypothesis 1.4. Hence, by Proposition 2.4, for each \( \sigma \in S^{\#} \) the multiplication defined on \( S \) by \( x \circ \sigma \circ y = x \circ y \) is a field multiplication. But choosing \( \sigma \) to be the multiplicative identity of \( S \) we have \( x \circ \sigma = x \circ y \) for all \( x, y \in S \). Thus the semifield must already have been a field, which is a contradiction.

3. Special 2-groups and the counter-examples

Suppose throughout this section that \( q = 2^{m} \). In [1] Beisiegel calls a special 2-group, \( P \), of order \( q^{3} \) with centre of order \( q \) ultraspecial if each quotient of \( P \) by a maximal subgroup of \( Z(P) \) is extraspecial.

The next result is cited in [1, Lemma 3] and is easily proven.

**Lemma 3.1.** Let \( p \) be a prime, \( L \cong GF(p^{m})^{+} \) and \( K \cong GF(p) \). Suppose that \( f : L \times L \to L \) is \( K \)-bilinear. Define a multiplication on \( P = P(f) = L \times L \times L \), by

\[
(a, b, c)(a', b', c') = (a + a', b + b', c + c' + f(a, b')).
\]

Then

(i) \( P \) is a group of nilpotence class at most 2;
(ii) the subgroups \( A = \{(a, 0, c) \mid a, c \in L\} \) and \( B = \{(0, b, c) \mid b, c \in L\} \) are elementary abelian; and
(iii) if for all elements \( a \in L \), \( \{f(a, l) \mid l \in L\} = \{f(l, a) \mid l \in L\} = L \), then \( P \) is ultraspecial.

**Lemma 3.2.** Assume that \( S \) is a pre-semifield of characteristic 2 and order \( q \) and that \( S_{\sigma} \) is the semifield built from \( S \) with \( \sigma \in S^{\#} \). Let \( Q \) and \( Q_{\sigma} \) be the quadratic functions constructed from \( S \) and \( S_{\sigma} \) via the procedure in Proposition 2.3. Then \( P(Q_{\sigma}) \cong P(Q) \).

**Proof.** First of all notice that \( Q \) and \( Q_{\sigma} \) are \( GF(2) \)-bilinear functions from \( S \times S \to S \). We consider the map

\[
\psi : P(Q_{\sigma}) \to P(Q),
\]

\[
(x \circ \sigma, \sigma \circ y, z) \mapsto (x, y, z).
\]

Then

\[
\psi((x \circ \sigma, \sigma \circ y, z)(x_1 \circ \sigma, \sigma \circ y_1, z_1))
\]

\[
= \psi(x \circ \sigma + x_1 \circ \sigma, \sigma \circ y + \sigma \circ y_1, z + z_1 + Q_{\sigma}(x \circ \sigma, \sigma \circ y_1))
\]

\[
= \psi((x + x_1) \circ \sigma, \sigma \circ (y + y_1), z + z_1 + (x \circ \sigma \circ y \circ y_1))
\]

\[
= \psi((x + x_1) \circ \sigma, \sigma \circ (y + y_1), z + z_1 + x \circ y_1)
\]

\[
= (x + x_1, y + y_1, z + z_1 + x \circ y_1) = (x, y, z)(x_1, y_1, z_1).
\]
So $\psi$ is a group homomorphism. Therefore, since $\psi$ is clearly surjective, $\psi$ is an isomorphism.

**Lemma 3.3.** Suppose that $L \cong GF(q)$ and $f : L \times L \to L$ is the bilinear form defined by $f((a,b)) = ab$. Then $P(f) \cong D(q)$.

**Proof.** See [1, Lemma 4].

**Lemma 3.4.** Suppose that $P$ is an ultraspecial 2-group of order $q^3$ and assume that there exist distinct elementary abelian subgroups $A$ and $B$ of $P$ of order $q^2$. Then

(i) $P = AB$ and $A \cap B = Z(P)$;

(ii) every involution of $P$ is contained in $A \cup B$;

(iii) if $x \in P \setminus Z(P)$ is an involution, then either $C_P(x) = A$ or $C_P(x) = B$;

(iv) the function $Q_P : P/Z(P) = P/N \to Z(P)$ defined by $Q_P(x) = x^2$ is a quadratic function. Moreover, $P = A \times B \cong K \times K$ where $K \cong GF(q)^+$ and the hypotheses (i) and (ii) of Proposition 2.4 are satisfied by $Q_P$ and $K$; and

(v) define $f_P : A \times B \to Z(P)$ by $f_P((a,b)) = Q_P(ab) = [a,b]$. Then $f_P$ is a $GF(2)$-bilinear function and $P \cong P(f_P)$.

**Proof.** Suppose that $x \in P \setminus Z(P)$ and $|C_P(x)| > q^2$. Then $|P : C_P(x)| < q$. Hence $|[P,x]| = [P : C_P(x)] < q$ and so there is a maximal subgroup $N$ of $Z(P)$ such that $|[P,x]| \leq N$. Therefore, $xN \in Z(P/N)$ and so, as $P$ is ultraspecial, $xN \in Z(P)/N$ which contradicts our initial selection of $x$. Therefore, (3.4.1) for each $x \in P \setminus Z(P)$, $|C_P(x)| \leq q^2$.

Suppose that $x \in A \cap B$. Then $C_P(x) \geq (A,B) > A$ and so, by (3.4.1), $x \in Z(P)$. Thus $A \cap B \leq Z(P)$ and consideration of group orders forces (i).

Now suppose that $x \in P \setminus A$ is an involution. Then, by (i), there exist $a \in A$ and $b \in B \setminus Z(P)$ such that $x = ab$. Now $1 = x^2 = abab = [a,b]$ which, since both $A$ and $B$ are elementary abelian, implies that $a \in C_P(b)$. But then $C_P(a) \geq (A,b)$ and (3.4.1) implies that $a \in Z(P) < B$. Hence $x \in B$ and (ii) holds and (iii) then follows from (3.4.1) and (ii).

The first part of (iv) is well-known (and easily checked) and then the hypotheses of Proposition 2.4 follow from (i)–(iii).

Finally we look at (v). We decompose $A = A_1 \times Z(P)$ and $B = B_1 \times Z(P)$. Then every element of $x \in P$ may be written uniquely as $a_1b_1z$ where $a_1 \in A_1$, $b_1 \in B_1$ and $z \in Z(P)$. Moreover, as $GF(2)$ vector spaces, $A_1 \cong B_1 \cong Z(P) \cong L$ where multiplication becomes addition. So we define a map

$$\theta : P \to P(f_P),$$

$$x = a_1b_1z \mapsto (b_1,a_1,z);$$

clearly $\theta$ is surjective. Suppose that $x = a_1b_1z_1$ and $y = a_2b_2z_2$ are elements of $P$. Then

$$xy = a_1b_1z_1a_2b_2z_2 = a_1b_2b_2z_1z_2 = a_1a_2b_1[b_1,a_2][b_2z_1z_2] = a_1a_2b_1b_2z_1z_2[b_1,a_2].$$

Therefore, $\theta(xy) = (b_1 + b_2, a_1 + a_2, z_1 + z_2 + f_P(b_1,a_2)) = \theta(x)\theta(y)$, and hence $P \cong P(f_P)$.

**Lemma 3.5.** Suppose that $P \cong D(q)$. Then $Q_P$ and $P/Z(P)$ satisfy Hypothesis 1.4.

**Proof.** A straightforward verification.
Theorem 3.6. The claims in [4, Corollary 2] and in [6, Lemmas (1.2), (1.3), (1.4) and Theorem (1.6)] are false.

Proof. Suppose that $S$ is a semifield and let $L = (S, +) \cong GF(q^2)$ and $V = L \times L$. Then, using Proposition 2.3, we can construct a quadratic function $Q : V \rightarrow L$ and a $GF(2)$-bilinear function $b : V \times V \rightarrow L$. We then can recover $S$ from $Q$ via the procedure in Proposition 2.4. Especially, as $S \cong S_{1s}$ as semifields, Proposition 2.4 implies that, if $S$ is chosen as a non-associative semifield, then $Q$ and $V$ do not satisfy Hypothesis 1.4. From here on we assume that $S$ is a non-associative semifield and construct $P = P(b)$ as in Lemma 3.1. Then, as $Q_P(=Q)$ does not satisfy Hypothesis 1.4, Lemma 3.5 implies that $P \not\cong D(q)$. Thus the claims in [4, Corollary 2] and in [6, Lemmas (1.2), (1.3), (1.4) and Theorem (1.6)] fail for $P$ and this completes the proof of Theorem 3.6.

For the readers who remain skeptical we now present generators and relations for a group of order $2^{15}$ which also proves the preceding theorem (and gives a quadratic function which is not a quadratic form).

Example 3.7. Let $I = \{1 \ldots 15\}$ and $P = \{x_i \mid x_i^2 = 1, i \in I\}$.

The above presentation was constructed using the GAP Computational Group Theory package [3] from the semifield multiplication on $GF(2^5)$ given by

\[
x \circ y = xy + (Tr_{GF(2^5)}(x)y + Tr_{GF(2)}(y)x)^2
\]

(see [2, page 243, statements (24) and 9]). That $P$ is not isomorphic to $D(2^5)$ is confirmed by observing, again using GAP, that the centralizer in $P$ of the element $x_1x_2x_11$ is non-abelian.

On the other hand we shall prove

Theorem 3.8. Suppose that $P$ is a $GF(q)$-type group of order $q^3$ and assume that for all involutions $x \in P \setminus Z(P)$, $C_P(x)$ is elementary abelian. If $P \setminus Z(P)$ contains involutions, then $P \cong D(q)$. 
Proof. Suppose that $P$ is of $GF(q)$-type and order $q^3$. Let $x \in P \setminus Z(P)$ be an involution. Then, by assumption and Definition 1.1 (i), $A = C_P(x)$ is elementary abelian of order $q^2$. Choose $y \in P \setminus A$. Then $[A, y] = Z(P)$, for otherwise, there exist $a_1, a_2 \in A \setminus Z(P)$ with $a_1 Z(P) \neq a_2 Z(P)$ and $[a_1, y] = [a_2, y]$ which implies $y \in C_P(a_1 a_2) = A$, by Definition 1.1 (ii), a contradiction. Suppose now that $y^2 \neq 1$. Then there exists $a \in A$ such that $y^2 = [a, y]$. Hence $(ya)^2 = y^2 a[a, y] = y^2 a^2 [a, y] = y^2 [a, y] = 1$ and so either $y$ or $ya$ is an involution. Therefore, without loss of generality we assume that $y^2 = 1$. Then, again by assumption and Definition 1.1 (i), $B = C_P(y)$ is elementary abelian of order $q^2$ and $A \neq B$. Furthermore, as, for all $x \in P \setminus Z(P)$, $[P : C_P(x)] = q$ we get $[x, P] = Z(P)$ for all $x \in P \setminus Z(P)$. Hence $P$ is ultraspecial and we may apply Lemma 3.4 to get that $P \cong P(f_P)$ where $f_P(\{\overline{a}, \overline{0}\}) = [a, b]$. Now because $P$ is of $GF(q)$-type, the quadratic function, $Q_P$, defined in Lemma 3.4 (vi) satisfies Hypothesis 1.4. Hence, Proposition 2.4 applies to $\overline{P} = P/\overline{Z(P)}$ and $Q_P$ to give $S \cong \overline{A} \cong \overline{B}$ the structure of a pre-semifield with multiplication defined by $\overline{x} \circ \overline{y} = Q_P(\overline{xy}) = f_P((\overline{x}, \overline{y})) = [x, y]$. Furthermore, for a fixed $a \in \overline{A}^\#$ we may construct a field $S_a$ and a quadratic form $Q_a$. However, by Lemma 3.2, $P(Q_a) = P(f_P) \cong P(Q_a)$ and, by Lemma 3.3, $P(Q_a) \cong D(q)$. Therefore, $P \cong P(f_P) \cong P(Q_a) \cong D(q)$ which completes the verification of Theorem 3.8.

4. Proof of Theorems 1.5 and 1.6

**Lemma 4.1.** Suppose that Hypothesis 1.4 holds. If $Q(v) \neq 0$ for all $v \in V^\#$, then $\dim_{GF(2)} V = 2m$.

**Proof.** Assume that $\dim_{GF(2)} V > 2m$. Then, by Hypothesis 1.3 (ii), $v^\perp > v^\perp \perp$ and so we may select $w \in v^\perp \setminus v^\perp \perp$. Suppose that $v_1, v_2 \in v^\perp \perp$ are such that $Q(v_1) = Q(v_2)$. Then $Q(v_1 + v_2) = b(v_1, v_2) + Q(v_1) + Q(v_2) = 0$, whence the hypothesis of the lemma implies that $v_1 = v_2$. Therefore, every element of $GF(q)^+$ is the image under $Q$ of some member of $v^\perp \perp$. In particular, there exists $x \in v^\perp \perp$ such that $Q(w) = Q(x)$. But then, as $w \in v^\perp \perp$ and $x \in v^\perp \perp \cap Q,$ $Q(w + x) = b(w, x) = Q(x) + Q(w) = b(w, x) = 0$, a contradiction. Thus $\dim_{GF(2)} V = 2m$, as predicted.

**Lemma 4.2.** Suppose that Hypothesis 1.3(iii) holds. Let $x \in U$. Then for all $y \in V \setminus x^\perp$, $x^\perp \perp \cap y^\perp = 0$.

**Proof.** Assume that $y \in V \setminus x^\perp$, $z \in x^\perp \perp \cap y^\perp$ and $z \neq 0$. Then $y \in z^\perp$. By Hypothesis 1.3 (iii), $z^\perp = x^\perp$ and so $y \in x^\perp$, contrary to our choice of $y$.

**Proof of Theorem 1.5.** Using Lemma 4.1 we may suppose that there exists $v \in V^\#$ with $Q(v) = 0$ (or else take $R = V$). By Hypothesis 1.4, $\dim_{GF(2)} V/v^\perp = m$ so there exists $w \in V \setminus v^\perp$. We construct a $GF(2)$-linear function $b_w : v^\perp \perp \to GF(q)^+$ via $b_w(x) = b(w, x)$. If $x, y \in v^\perp \perp$ with $x \neq y$ satisfy $b_w(x) = b_w(y)$, then $b_w(x) + b_w(y) = 0$ and hence $b(w, x - y) = 0$. Therefore, as $(x - y)^\perp = v^\perp$ by Hypothesis 1.3(iii), $w \in v^\perp$ which is against our initial choice of $w$. Hence we conclude that $b_w$ is a bijective $GF(2)$-linear transformation from $v^\perp \perp$ to $GF(q)^+$.

Suppose that $Q(w) \neq 0$. Then we may pick $v_1 \in v^\perp \perp$ such that $Q(w) = b_w(v_1) = b(w, v_1)$. This gives $Q(v_1 + w) = Q(v_1) + Q(w) + b(v_1, w) = Q(v_1).$ Now
using Hypothesis 1.3(iv) we get that \( Q(v_1 + w) = Q(v_1) = 0 \). Thus we may suppose that \( w \in V \setminus \bar{v}^\perp \) is chosen so that \( Q(w) = 0 \).

Set \( V_1 = v_1^\perp + w_1^\perp \). Observe that by Lemma 4.2 and Hypothesis 1.3(ii), \( w_1^\perp = w_1^\perp + (v_1^\perp \cap w_1^\perp) \) and \( v_1^\perp = v_1^\perp + (v_1^\perp \cap w_1^\perp) \). Therefore, \( V = (v_1^\perp + w_1^\perp) + (v_1^\perp \cap w_1^\perp) \). Hence as \( V_1^\perp \cap V_1 = 0 \) and \( V_1^\perp \supseteq (v_1^\perp \cap w_1^\perp) \), we get \( V = V_1 \perp V_1^\perp \). Now we show that both \( V_1 \) and \( V_1^\perp \) satisfy Hypothesis 1.3. Clearly Hypothesis 1.3(i) holds for both subspaces. Suppose that \( z \in V_1 \). Then \( z^\perp \supseteq V_1^\perp \) and so the first part of Hypothesis 1.3(ii) holds for \( V_1 \) and similarly it holds for \( V_1^\perp \). Suppose that \( z_1 \in z^\perp \). Then there exists \( x \in V_1 \) and \( k \in V_1^\perp \) so that \( z_1 = x + k \). Then for all \( l \in V_1^\perp \), \( b(z_1, l) = b(x + k, l) = b(x, l) + b(k, l) = b(k, l) \). Since, by Hypothesis 1.3(iii), \( z_1^\perp = z^\perp \supseteq V_1^\perp \) we get \( 0 = b(z, l) = b(z_1, l) = b(k, l) \). This is true for all \( l \in V_1^\perp \) whence \( k \in V_1^\perp = V_1 \) and so \( k \in V_1 \cap V_1^\perp = 0 \). Therefore, \( z^\perp \subseteq V_1 \). A similar argument shows that if \( z \in V_1^\perp \), then \( z^\perp \subseteq V_1 \). This shows that Hypothesis 1.3(ii) holds. The validity of Hypothesis 1.3(iii) and Hypothesis 1.3(iv) for \( V_1 \) and \( V_1^\perp \) immediately follow from Hypothesis 1.3(ii).

Now, by construction, \( Q(V_1) \neq 0 \). We proceed by induction so long as there is a non-zero \( V_1^\perp \) with \( Q(V_1^\perp) \neq 0 \). Thus we decompose \( V \) into an orthogonal sum of \( 2m \)-dimensional spaces each satisfying Hypothesis 1.4 and a further space, \( X \) which, if it is non-zero, satisfies Hypothesis 1.3 with \( Q(X) = 0 \). Finally, in the case that \( X \) is non-zero Lemma 4.1 gives us the result.

**Proof of Theorem 1.6.** The function \( Q : P/Z(P) \to Z(P) \) given by squaring the elements of \( P \) is a quadratic function and, as \( P \) is of \( GF(q) \)-type, Hypothesis 1.4 is satisfied for \( Q \) and \( V = P/Z(P) \). Hence, by Theorem 1.5, \( (P/Z(P), Q) \) decomposes as an orthogonal sum of vector spaces \( V_1 \) of dimension \( 2m \) each of which satisfies Hypothesis 1.3. Moreover, \( Q(V_1) \neq 0 \) for all but at most one of the orthogonal summands. Reinterpreting this back in \( P \) we have decomposed \( P \) into a central product of groups of order \( q^3 \) each of which is of \( GF(q) \)-type and all but at most one of the factors contains an involution outside of \( Z(P) \). Now, by Theorem 3.8, each of the factors which contains an involution outside of \( Z(P) \) is isomorphic to \( D(q) \). Thus it only remains to discover the type of the remaining factor (if there is one).

Now, by Proposition 2.4, we can give a field structure to and define a quadratic form on each orthogonal summand in \( P/Z(P) \) which satisfies Hypothesis 1.4. This means that the space \( P/Z(P) \) satisfies the conclusions of [4, Lemma 2.1]. So we can follow Stroth [4, Section 2] to show that the remaining factor also admits a field structure and a definite quadratic form. Then using the last part of [4, Lemma 3.1 (last page only)] or [1, Satz 3] we find that the remaining factor is either trivial or is isomorphic to a Sylow 2-subgroup of \( SU_3(q) \) as desired.

**References**

    MR 80f:20020

School of Mathematics and Statistics, University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom
E-mail address: cwp@for.mat.bham.ac.uk

Department of Mathematics, University of Manchester Institute of Science and Technology, P.O. Box 88, Manchester M60 1QD, United Kingdom
E-mail address: Peter.Rowley@umist.ac.uk