Bull. Aust. Math. Soc. **84** (2011), 393–407
doi:10.1017/S0004972711002474

ON $B(5, k)$ GROUPS

YUANLIN LI✉ and XIAOYING PAN

(Received 30 November 2010)

Abstract

A group G is said to be a $B(n, k)$ group if for any n-element subset A of G, $|A^2| \le k$. In this paper, characterizations of $B(5, 16)$ groups and $B(5, 17)$ groups are given.

2010 *Mathematics subject classification*: primary 20D60; secondary 20E34.
Keywords and phrases: small squaring property, $B(n, k)$ groups.

1. Introduction

A group G is said to have the small squaring property on n-element subsets if for any n-element subset A of G, $|A^2| < n^2$, where $A^2 = \{ab \mid a, b \in A\}$. Furthermore, G is called a B_n-group if $|A^2| \le \frac{1}{2}n(n+1)$ for all n-element subsets A. Recently, Eddy and Parmenter generalized these notions to a new notion of $B(n, k)$ groups [3]. A group G is called a $B(n, k)$ group if $|A| = n$ implies $|A^2| \le k$ with $k \le n^2 - 1$. Therefore a B_n-group is a $B(n, \frac{1}{2}n(n+1))$ group, and a group with small squaring property on n-element subsets is a $B(n, n^2 - 1)$ group.

Determining all $B(n, k)$ groups is an interesting problem. For any given k, G is obviously a $B(n, k)$ group when $|G| \le k$, and such G is referred to as *trivial*. It is also easy to see that any abelian group G is a $B(n, k)$ group when $k \ge \frac{1}{2}n(n+1)$. So what we are interested in is to determine all nonabelian nontrivial $B(n, k)$ groups.

The $B(n, k)$ groups for $n = 2$ and $n = 3$ have been completely characterized in the literature [1, 3, 4, 9, 10]. For $n = 4$, all $B(4, 10)$ groups were characterized by Parmenter in [10], and $B(4, k)$ groups where $k = 11, 12$, and 13 were recently characterized by Li and Tan in [7, 8]. The only known result for $B(5, k)$ groups with $k \ge 15$ is the characterization of $B(5, 15)$ groups given by Li and Tan in [6], and it was shown that G is a nonabelian nontrivial $B(5, 15)$ group if and only if $G \cong Q_8 \times C_2$. In this paper, we continue the investigation on $B(5, k)$ groups for $k = 16$ and 17. We provide the complete characterizations of $B(5, 17)$ non-2-groups and 2-groups in Sections 2 and 3, respectively. In Section 4 we obtain a complete characterization

This research was supported in part by a Discovery Grant from the National Sciences and Engineering Research Council of Canada.

of $B(5, 16)$ groups, and we also give a short proof for the characterization of $B(5, 15)$ groups.

Throughout the paper, all nonabelian groups are assumed to be finite, and our notation for groups is standard and follows that in [11]. In particular, we denote the quaternion group of order eight and the dihedral group of order $2n$ by Q_8 and D_{2n}, respectively:

$$Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1}\rangle,$$
$$D_{2n} = \langle a, b \mid a^n = b^2 = 1, a^b = a^{-1}\rangle.$$

2. The characterization of $B(5, 17)$ non-2-groups

In this section, we investigate $B(5, 17)$ non-2-groups. We first work on a necessary condition for a non-2-group G to be a $B(5, 17)$ group. Afterwards, we will give a complete characterization of $B(5, 17)$ non-2-groups. Throughout the section, a group G is assumed to be a non-2-group.

2.1. A necessary condition for $B(5, 17)$ non-2-groups. We first characterize a Sylow subgroup of odd order of a $B(5, 17)$ group.

LEMMA 2.1. *Let P be a Sylow subgroup of odd order of a $B(5, 17)$ group G. Then P is abelian.*

PROOF. Suppose on the contrary that P is not abelian. Then P has two maximal subgroups M and N containing $Z(P)$. Let $L = M \cap N$, and hence $Z(P) \subseteq L$. It was proved in [1] that there exist $a \in M - L$ and $b \in N - L$ such that $ab \neq ba$.

Let $A = \{a, b, ab, b^2, ab^2\}$. Then A^2 contains a subset

$$B = \{a^2, a^2b, ab^2, a^2b^2, ba, b^2, bab, b^3, bab^2, aba, abab, ab^3, abab^2, b^2a, b^2ab, b^4, b^2ab^2, ab^2a, ab^2ab, ab^4, ab^2ab^2\}.$$

Since M and N are maximal subgroups of P, $M \lhd P$ and $N \lhd P$. Since N, aN and a^2N are disjoint, we may write B as a disjoint union of subsets, that is,

$$B = (B \cap N) \cup (B \cap aN) \cup (B \cap a^2N)$$

where

$$B \cap N = \{b^2, b^3, b^4\},$$
$$B \cap aN = \{ab^2, ab^3, b^2a, b^2ab, b^2ab^2, ab^4, ba, bab, bab^2\} \quad \text{and}$$
$$B \cap a^2N = \{a^2, a^2b, a^2b^2, aba, abab, abab^2, ab^2a, ab^2ab, ab^2ab^2\}.$$

To show that the 21 elements in B are distinct, we only need to verify that the elements in each subset above are distinct.

In $B \cap N$, since the order of b is odd, the three elements are distinct.

In $B \cap aN$, $\{ab^2, b^2a, bab\} \subseteq b^2M$, $\{ab^3, b^2ab, bab^2\} \subseteq b^3M$, and $\{b^2ab^2, ab^4, ba\} \subseteq bM \cup b^4M$. Since the subsets b^2M, b^3M, $bM \cup b^4M$ are disjoint, we only need to show that the elements in each subset are distinct. Since the order of b is odd, $ab^2 \neq b^2a$. It is not hard to show that those three elements in each subset are distinct and thus the nine elements in $B \cap aN$ are distinct.

In $B \cap a^2N$, $\{a^2, abab^2, ab^2ab\} \subseteq M \cup b^3M$, $\{a^2b, aba, ab^2ab^2\} \subseteq bM \cup b^4M$, and $\{a^2b^2, abab, ab^2a\} \subseteq b^2M$. Similar to above, we can show that the nine elements in $B \cap a^2N$ are distinct.

Therefore $|B| = 3 + 9 + 9 = 21$, and thus G is not a $B(5, 17)$ group, giving a contradiction. So P is abelian. □

Lemma 2.2. *Let G be a $B(5, 17)$ group of odd order. Then G is abelian.*

Proof. Suppose on the contrary that there exists some finite nonabelian $B(5, 17)$ group of odd order and let G be such a group with minimal order. It follows from Lemma 2.1 that G is not nilpotent. Since all proper subgroups of G are abelian, G is a minimal nonnilpotent group. It follows from [11, Theorem 9.1.9] that $|G| = p^uq^v$, where p and q are distinct primes. Moreover, G has a normal Sylow q-subgroup Q and a nonnormal cyclic Sylow p-subgroup P, say $P = \langle a\rangle$. Since P is not a normal subgroup of G, there exists $b \in Q$ such that $a^b \notin \langle a\rangle$; in particular, $ab \neq ba$. We next divide the proof into two cases according to whether $|P| > 3$ or $|P| = 3$.

Case 1: $|P| > 3$. Let $A = \{b, a, ba^2, a^2, ba\}$. Note that A^2 contains a subset

$$B = \{b^2, ba, b^2a^2, ba^2, ab, a^2, aba^2, a^3, ba^2b, ba^3, ba^2ba^2, ba^4, ba^2ba, a^2ba^2, a^4, a^2ba, bab, baba^2, baba\}.$$

Recall that $Q \lhd G$. Then we get $B \cap Q = \{\underline{b^2}\}$, $B \cap aQ = \{\underline{ba}, \underline{ab}, \underline{bab}\}$, $B \cap a^2Q = \{\underline{b^2a^2}, \underline{ba^2}, \underline{a^2}, \underline{ba^2b}, \underline{baba}\}$, $B \cap a^3Q = \{\underline{aba^2}, \underline{a^3}, \underline{ba^3}, \underline{a^2ba}, ba^2ba, baba^2\}$, and $B \cap a^4Q = \{\underline{ba^2ba^2}, \underline{ba^4}, \underline{a^2ba^2}, \underline{a^4}\}$. Since subsets $B \cap Q$, $B \cap aQ$, $B \cap a^2Q$, $B \cap a^3Q$ and $B \cap a^4Q$ are disjoint, we just need to find distinct elements in each subset. Note that $a^2b \neq ba^2$. And by this condition, we also have $a \neq bab$ and $a^2 \neq ba^2b$ $(*)$. (If $a = bab$ (that is, $b^a = b^{-1}$), then $b^{a^2} = (b^{-1})^a = b$, which is a contradiction. Similarly, if $a^2 = ba^2b$ (that is, $b^{a^2} = b^{-1}$), then $b^{a^4} = (b^{-1})^{a^2} = b$, which means that $ba = ab$, and this is a contradiction.) By $(*)$, it is easy to know that the 17 underlined elements above are distinct. Since G is a $B(5, 17)$ group, ba^2ba in $B \cap a^3Q$ must be a redundant element. The only possibility is $ba^2ba = aba^2$. A similar argument shows that $baba^2 = a^2ba$. From these two equations, we get $ba^2b = aba$ and $baba = a^2b$. Then $aba = ba^2b = b^2aba$, from which we get $b^2 = 1$, giving a contradiction.

Case 2: $|P| = 3$. We first assume that $ba = ab^2$. Recall that $o(a) = 3$, $b = a^{-3}ba^3 = b^8$, and thus $o(b) = 7$. Let $A = \{a, b^2, ab, a^2b^3, b^3\}$. Then

$$A^2 = \{a^2, ab^2, a^2b, b^3, ab^3, ab^4, b^4, ab^5, a^2b^4, b^5, a^2b^2, a^2b^3, 1, b^6, a^2b^5, ab, a^2b^6, ab^6, a\}.$$

Since $A^2 \cap Q$, $A^2 \cap aQ$, and $A^2 \cap a^2Q$ are disjoint, and the elements in each subset are distinct, we know that $|A^2| = 19$, which is a contradiction. Thus, $ba \neq ab^2$. By replacing a with a^2 in the above argument, we can show that $ba^2 \neq a^2b^2$, that is, $ab \neq b^2a$. We can also show that $a^{-1}ba \neq b^{-2}$ (otherwise, we have $o(b) = 9$ which

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

is not co-prime to $o(a)$, giving a contradiction). If $a^{-1}ba = b^3$, then $o(b) = 13$. Let $A = \{a, b^2, ab, a^2b^3, b^3\}$. Then

$$A^2 = \{b^3, b^4, b^5, b^6, b^9, b^{10}, b^{12}, ab^2, ab^3, ab^4, ab^6, ab^7, ab^9, ab^{10}, a^2, a^2b, a^2b^3, a^2b^4, a^2b^5, a^2b^6, a^2b^8\}.$$

So $|A^2| = 21$, giving a contradiction. Similarly, it is not hard to prove that $a^{-1}ba \neq b^k$, where $k = 0, \pm1, \pm2, \pm3, \pm4$ $(**)$. Let $A = \{a, b, ab, ab^2, ab^3\}$. Then A^2 contains a subset

$$B = \{b^2, ab, ba, bab, bab^2, bab^3, ab^2, ab^3, ab^4, a^2, abab, a^2b, a^2b^2, a^2b^3, aba, abab^2, abab^3, ab^2ab\}.$$

Using the condition $(**)$, it is not hard to show that the elements in B are distinct, and thus $|B| = 18$, which gives a contradiction.

In both cases above, we have found contradictions. Therefore any finite $B(5, 17)$ group G of odd order is abelian. □

Lemma 2.3. *Let G be a nontrivial $B(5, 17)$ non-2-group with a nontrivial Sylow 2-subgroup P. Then G has a normal subgroup T of odd order such that $G = TP$.*

Proof. Assume to the contrary that G is a $B(5, 17)$ group which does not have a normal subgroup of odd order with 2-power index. Let H be a subgroup of G with minimal order such that it does not have a normal subgroup of odd order with 2-power index. Then every proper subgroup of H has a normal subgroup of odd order with 2-power index. It follows from [5, Ch. IV, Theorem 5.4] that a Sylow 2-subgroup P_1 of H is normal in H and its exponent is at most 4. Moreover, $|H/P_1| = q^{\nu}$ for some odd prime q and a Sylow q-subgroup T of H is cyclic, say $T = \langle a\rangle$. Since T is not normal in H, there exists an element $b \in P_1$ such that $a^b \notin \langle a\rangle$, in particular, $ab \neq ba$.

We first assume that $|H| \leq 17$. By checking all the groups of order up to 17 which satisfy the above-mentioned properties, we know that $H \cong A_4$. Let $a \in T$ and $b \in P_1$ be the elements of H corresponding to the elements (123) and (12)(34) of A_4, respectively. Since $|G| \geq 18$, there exists another element $c \in G - H$. Since $ab \neq ba$, by replacing c with ac, bc, or abc if necessary, we can assume that $bc \neq cb$, $ac \neq ca$. Let $A = \{a, b, ab, a^2b, c\}$. Then A^2 has a subset

$$\begin{aligned} B &= (B \cap H) \cup (B \cap (G - H)) \\ &= \{\underline{a^2}, \underline{ab}, \underline{a^2b}, \underline{b}, \underline{ba}, \underline{1}, \underline{bab}, \underline{aba}, \underline{a}, \underline{abab}, \underline{aba^2b}, \underline{a^2bab}\} \\ &\quad \cup \{\underline{ac}, \underline{bc}, \underline{abc}, \underline{a^2bc}, \underline{cb}, ca, cab\}. \end{aligned}$$

A straightforward computation shows that the 17 underlined elements in B are distinct. Next, we consider elements ca and cab. It is not hard to see that ca is different from ac, bc, cb and cab; cab is different from bc, ca and cb. Since G is a $B(5, 17)$ group, we may assume that ca is a redundant element. If $ca = abc$, we note that cab can only be equal to ac or a^2bc. If $cab = ac$, then $cab = abcb = ac$, which leads to $bcb = c$. Since b corresponds to (12)(34), that is, $o(b) = 2$, we get $cb = bc$ from the above equation, which is a contradiction. If $cab = a^2bc$, then $abcb = a^2bc$, which leads to $bcb = abc$, that is, $cbc^{-1} = b^{-1}ab$. Since $o(cbc^{-1}) = 2$, while $o(b^{-1}ab) = 3$, this gives a contradiction. We have shown that both cases are impossible. Thus $ca \neq abc$. If $ca = a^2bc$, we note that cab can only be equal to ac or abc. Similarly, we can show that both cases are impossible. Therefore we conclude that $|A^2| \geq 18$, and thus G is not a $B(5, 17)$ group, giving a contradiction.

Next, assume that $|H| \geq 18$. Without loss of generality, we may assume that $H = G$. Let b be an element of maximal order in P such that $ab \neq ba$. As before, we also know that $a^2b \neq ba^2$. We divide the proof into two cases according to the order of a.

Case 1: $o(a) > 3$. Let $A = \{a, b, ab, a^{-1}b, a^2\}$. Then

$$\begin{aligned} A^2 \cap P &\supseteq \{\underline{b}, \underline{b^2}, \underline{a^{-1}ba}, \underline{a^{-1}bab}, aba^{-1}b\}, \\ A^2 \cap aP &\supseteq \{\underline{ab}, \underline{ba}, \underline{bab}, \underline{ab^2}\}, \\ A^2 \cap a^2P &\supseteq \{\underline{a^2}, \underline{a^2b}, \underline{aba}, \underline{ba^2}\}, \\ A^2 \cap (a^3P \cup a^{-2}P) &\supseteq \{\underline{a^{-1}ba^{-1}b}, \underline{a^3}, \underline{a^3b}, aba^2\}, \\ A^2 \cap (a^{-1}P \cup a^4P) &\supseteq \{\underline{ba^{-1}b}, \underline{a^4}\}. \end{aligned}$$

Since $P \triangleleft G$ and subsets P, aP, a^2P, $a^3P \cup a^{-2}P$ and $a^{-1}P \cup a^4P$ are disjoint, it is not hard to show that the 17 underlined elements above are distinct. Next we show that there must be another distinct element in A^2. If $o(a) > 5$, it is easy to see that aba^2 is the 18th distinct element. If $o(a) = 5$, we consider $aba^{-1}b$ in $A^2 \cap P$. If $aba^{-1}b$ is not a redundant element, it is the 18th distinct element. We may assume $aba^{-1}b$ is a redundant element. Note that the only possibility is $aba^{-1}b = a^{-1}ba$. Then $a^{-1}ba^{-1}b = a^{-2}aba^{-1}b = a^{-3}ba = a^2ba$, which is different from aba^2. So aba^2 is the 18th distinct element under this circumstance. Therefore $|A^2| \geq 18$, and thus G is not a $B(5, 17)$ group, giving a contradiction.

Case 2: $o(a) = 3$. Suppose first that $o(b) = 4$. Let $A = \{a, b, ab, ab^{-1}, a^2\}$. Then A^2 contains a subset

$$\begin{aligned} B &= (B \cap P) \cup (B \cap aP) \cup (B \cap a^2P) \\ &= \{\underline{1}, \underline{b^{-1}}, \underline{b}, \underline{b^2}, \underline{aba^2}, \underline{ab^{-1}a^2}\} \cup \{\underline{ab}, \underline{ba}, \underline{bab}, \underline{bab^{-1}}, \underline{ab^2}, \underline{a}\} \\ &\quad \cup \{\underline{a^2}, \underline{a^2b}, \underline{a^2b^{-1}}, ba^2, \underline{aba}, \underline{abab}, \underline{abab^{-1}}, \underline{ab^{-1}a}, ab^{-1}ab, ab^{-1}ab^{-1}\}. \end{aligned}$$

We first show that $a \neq bab$, that is, $a^{-1}ba \neq b^{-1}$. Otherwise, $b^{a^2} = b$, and then $ab = ba$, giving a contradiction. Recall that $ba \neq ab^2$. Since P, aP and a^2P are disjoint, it is not hard to show that the 19 underlined elements in B are distinct. Thus $|B| \geq 19$, giving a contradiction.

Therefore $o(b) = 2$, and then P is elementary abelian. Since $|G| \geq 18$ and $|T| = 3$, $|P| \geq 8$. Then we can choose an element $c \in P$ such that $c \notin \langle b^a, b\rangle \cup \langle b^{a^2}, b\rangle = K$. Note that $bc \notin K$. Replacing c by bc if necessary, we can assume that $ac \neq ca$. Let $A = \{a, b, ab, ac, bca^2\}$. Then A^2 contains a subset

$$B = \{a^2, ab, a^2b, a^2c, ba, 1, bab, bac, aba, a, acb, abab, abac, aba^2, bc, b, c\}.$$

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

As before, we can show that $|B| = 17$. We next show that at least one of $abca^2$ and aca^2 in A^2 is a new distinct element. Otherwise, if both are in B, we note that both must be in $\{bc, c, b\}$. If $aca^2 \notin \{bc, c, b\}$, then aca^2 is the 18th distinct element. So we assume that $aca^2 \in \{b, c, bc\}$. If $aca^2 = b$, then $c = a^{-1}ba$, which contradicts $c \notin K$. If $aca^2 = c$, then $ac = ca$, which is a contradiction. If $aca^2 = bc$, since $abca^2 \notin \{aca^2, 1\}$, $abca^2$ can only be equal to b or c. If $abca^2 = c$, then $c = aba^{-1}aca^2 = aba^{-1}bc$, and we get $ab = ba$, which is a contradiction. If $abca^2 = b$, then $c = ba^{-1}ba$, which contradicts $c \notin K$.

Therefore $|A^2| \geq 18$, and thus G is not a $B(5, 17)$ group, giving a contradiction. □

In what follows, we assume that G is a nontrivial nonabelian $B(5, 17)$ non-2-group having a Sylow 2-subgroup P and the normal 2-complement T.

Lemma 2.4. *T is abelian and not centralized by P.*

Proof. It follows from Lemma 2.2 that T is abelian. Suppose that P centralizes T. Then $G = P \times T$ and since G is not abelian, P is not abelian. It is easy to see that P has two distinct maximal normal subgroups M and N containing $Z(P)$. Similar to the proof in Lemma 2.1, we have two elements $a \in M - N$ and $b \in N - M$ such that $ab \neq ba$. Let $A = \{a, b, bc, abc, abc^2\}$ where $c \in T - \{1\}$. If $a^2 \neq b^2$, A^2 contains a subset

$$\begin{aligned} B &= (B \cap (N \times T)) \cup (B \cap a(N \times T)) \\ &= \{a^2, a^2bc, a^2bc^2, b^2, abac, ababc^2, abac^2, ababc^4\} \\ &\qquad \cup \{ab, abc, ba, babc, babc^2, bac, babc^3, ab^2c, ab^2c^2, ab^2c^3\}. \end{aligned}$$

Since subsets $N \times T$ and $a(N \times T)$ are disjoint, it is not hard to show that the 18 elements in B are distinct. If $a^2 = b^2$, then

$$\begin{aligned} A^2 &= (A^2 \cap (N \times T)) \cup (A^2 \cap a(N \times T)) \\ &= \{\underline{a^2}, \underline{a^2bc}, \underline{a^2bc^2}, \underline{b^2c}, \underline{b^2c^2}, \underline{abac}, ababc^2, ababc^3, \underline{abac^2}, ababc^4\} \\ &\qquad \cup \{\underline{ab}, \underline{abc}, \underline{ba}, \underline{babc}, \underline{babc^2}, \underline{bac}, \underline{babc^3}, \underline{ab^2c}, \underline{ab^2c^2}, \underline{ab^2c^3}\}. \end{aligned}$$

As before, it is easy to show the 17 underlined elements are distinct. Since G is a $B(5, 17)$ group, we know that $ababc^2$, $ababc^3$ and $ababc^4$ must be redundant elements. Therefore we get $a = bab$, $b = aba$ and $o(c) = 3$, so $o(a) = o(b) = 4$. Let $A_1 = \{a, ab, bc, abc, bac^2\}$. Then

$$A_1^2 = \{a^2, a^2b, b, a^3, 1, a, abc, a^2bc, a^2c, ac, bac, bc, a^3c, bc^2, a^3c^2, a^2c^2, ac^2, b^3c^2, c^2\}.$$

It is easy to show that the 19 elements in A_1^2 are distinct. Thus G is not a $B(5, 17)$ group, giving a contradiction. □

Lemma 2.5. *P has a subgroup Q of index 2 which centralizes T and every element of $P - Q$ inverts T.*

Proof. We first show that for each $b \in P$ either b centralizes T or b inverts T. Assume that $b \in P$ does not centralize T. So $ab \neq ba$ for some $a \in T$. First we show

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

that $b^2a = ab^2$. Assume to the contrary that $b^2a \neq ab^2$. Then $o(b) \geq 4$. Let $A = \{a, ab, ab^2, ab^3, 1\}$. Then A^2 contains a subset

$$B = \{a^2, abab^3, ab^2ab^2, ab^3ab, 1, a^2b, aba, ab^2ab^3, ab^3ab^2, a^2b^2, abab, ab^2a, ab^3ab^3, a^2b^3, abab^2, ab^2ab, ab^3a, ab^3\}.$$

Since $T \lhd G$, $ab \neq ba$ and $b^2a \neq ab^2$, as before, it is not difficult to show that the 18 elements in B are distinct, and thus G is not a $B(5, 17)$ group, giving a contradiction. So $b^2a = ab^2$.

We now prove that $b^{-1}ab = a^{-1}$. Assume to the contrary that $b^{-1}ab \neq a^{-1}$. We first assume that $o(b) \geq 4$. Let $A = \{a, ab, a^2b, ab^2, b^2\}$. Then A^2 contains a subset

$$B = \{a^2, ab^4, b^4, a^2b, a^3b, aba, a^2ba, a^2b^2, ab^2, abab, aba^2b, a^2bab, a^2ba^2b, abab^2, a^2b^3, ab^3, a^3b^3, a^2bab^2\}.$$

We first show that $ba \neq a^2b$. Otherwise $bab^{-1} = a^2$. Since $b^2a = ab^2$, $a = b^2ab^{-2} = a^4$. Therefore $o(a) = 3$, and then $bab^{-1} = a^{-1}$, contradicting the assumption. Similarly, we have $ab \neq ba^2$ and $b^{-1}ab \neq a^{-2}$. In view of these facts, it is not hard to show that the 18 elements in B are distinct. Thus $|A^2| \geq 18$, and then G is not a $B(5, 17)$ group, giving a contradiction. Next assume that $o(b) = 2$. Let $A = \{a, ab, a^2b, b, a^{-1}\}$. Then A^2 contains a subset

$$B = \{1, a, a^2, bab, abab, a^2bab, ba^2b, aba^2b, a^2ba^2b, ab, a^2b, a^3b, aba^{-1}, aba, a^2ba^{-1}, a^2ba, ba^{-1}, ba\}.$$

As in the proof of Lemma 2.2, we can show that $b^{-1}ab = bab \neq a^k$, where $k = 0, \pm1, \pm2, \pm3$, and thus the elements in B are distinct. So $|A^2| \geq 18$, which means that G is not a $B(5, 17)$ group, giving a contradiction. Thus we have $b^{-1}ab = a^{-1}$.

Next we show that b inverts T. Note that we just showed that for each $y \in T$ either $y^b = y$ or $y^b = y^{-1}$. Suppose that there exists $x \in T - \{1\}$ such that $x^b = x$. Since $xa \in T$, we have either $(xa)^b = xa$ or $(xa)^b = (xa)^{-1}$. The former leads to $xa^{-1} = (xa)^b = xa$, and then $a^2 = 1$, giving a contradiction. The latter gives that $xa^{-1} = (xa)^b = (xa)^{-1} = a^{-1}x^{-1} = x^{-1}a^{-1}$, and then $x^2 = 1$, again giving a contradiction. Therefore b inverts T.

Set $Q = \{g \in P \mid t^g = t \text{ for all } t \in T\}$. Clearly Q is a subgroup of P which centralizes T and every element b of $P - Q$ does not centralize T. So by what we just proved, b inverts T. It remains to show that $[P : Q] = 2$. It follows from Lemma 2.4 that $P \neq Q$, so there exists $b \in P - Q$. Since for every element $b' \in P - Q$, b' inverts T, we have $b'b \in Q$. Thus $b' \in Qb^{-1}$, proving $[P : Q] = 2$. □

In the following lemma, Q will denote a subgroup of P of the type determined in Lemma 2.5.

Lemma 2.6. *P is abelian, and the exponent of Q is at most 2.*

Proof. Suppose on the contrary that P is not abelian. Then there exist elements $a \in Q$ and $b \in P - Q$ such that $ab \neq ba$. Otherwise, if each element $b \in P - Q$ centralizes Q, then b centralizes $\langle b, Q\rangle$. Since $[P : Q] = 2$ and $b \notin Q$, $\langle b, Q\rangle = P$, so $b \in Z(P)$.

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Thus $P - Q \subseteq Z(P)$. Since $P = \langle P - Q\rangle \subseteq Z(P)$, P is abelian, giving a contradiction. If $a^2 \neq 1$, let $A = \{b, ba, t, a, at\}$ where $t \in T - \{1\}$. Then A^2 contains a subset

$$\begin{aligned} B &= (B \cap (Q \times T)) \cup (B \cap b(Q \times T)) \\ &= \{\underline{b^2}, \underline{b^2a}, \underline{bab}, baba, \underline{t^2}, \underline{ta}, \underline{tat}, \underline{a^2t}, \underline{a^2t^2}\} \\ &\quad \cup \{\underline{bt}, \underline{ba}, \underline{bat}, \underline{ba^2}, \underline{ba^2t}, \underline{tb}, \underline{tba}, \underline{ab}, \underline{aba}, \underline{atb}\}. \end{aligned}$$

It is easy to show the 18 underlined elements in B are distinct, giving a contradiction. Thus $a^2 = 1$. If $b^2 = 1$, since $ab \neq ba$, we have $(ab)^2 \neq 1$. Replacing b by ab if necessary, we may assume that $b^2 \neq 1$. Let $A_1 = \{b, ba, t, a, bt\}$. Then

$$\begin{aligned} A_1^2 &= (A_1^2 \cap (Q \times T)) \cup (A_1^2 \cap b(Q \times T)) \\ &= \{\underline{b^2}, \underline{b^2a}, \underline{bab}, baba, \underline{1}, \underline{b^2t}, \underline{babt}, at, \underline{t^2}, \underline{b^2t^{-1}}, \underline{b^2at^{-1}}\} \\ &\quad \cup \{\underline{ba}, \underline{ba^2}, b, \underline{ab}, \underline{aba}, \underline{bt}, \underline{bat}, \underline{abt}, \underline{bt^{-1}}, \underline{bat^{-1}}, bt^2\}. \end{aligned}$$

It is not hard to show that the 18 underlined elements here are distinct, so that $|A_1^2| \geq 18$, giving a contradiction. Therefore P must be abelian.

Next we will show that the exponent of Q is at most 2. Suppose on the contrary that Q contains an element a of order four. Let $b \in P - Q$ and $t \in T - \{1\}$. By replacing b with ba if necessary, we can assume that $o(b) \geq 4$. Consider $A = \{t, at^{-1}, tab, bt, a^2b\}$. Then A^2 contains a subset

$$\begin{aligned} B = \{&b, ab, a^2b, b^2, a^2b^2\} \cup \{a^3bt, a^2b^2t, a^3b^2t, abt^{-2}, a^2bt^{-2}, ab^2t^{-2}\} \\ &\cup \{bt^2, abt^2, ab^2t^2, a^2bt^{-1}, a^3bt^{-1}, a^2b^2t^{-1}, a^3b^2t^{-1}\}. \end{aligned}$$

It is not hard to show that the 18 elements in B are distinct. Therefore G is not a $B(5, 17)$ group, giving a contradiction. So the exponent of Q is at most 2. □

Summarizing the results proved in the above lemmas, we obtain a necessary condition for $B(5, 17)$ non-2-groups.

Theorem 2.7. *Let G be a nontrivial nonabelian $B(5, 17)$ non-2-group. Then $G = TP$ where T is a normal abelian subgroup of odd order and P is a nontrivial abelian Sylow 2-subgroup of G. Furthermore, the subgroup $Q = C_P(T)$ has index 2 in P, the exponent of Q is at most 2, and each element of $P - Q$ inverts T.*

2.2. A complete characterization of $B(5, 17)$ non-2-groups. In this subsection, we complete the characterization of $B(5, 17)$ non-2-groups, and show that there is no nontrivial nonabelian $B(5, 17)$ non-2-group.

Lemma 2.8. *D_{2n} with $n \geq 9$ is not a $B(5, 17)$ group.*

Proof. We have $D_{2n} = \langle a, x \mid a^n = x^2 = 1, a^x = a^{-1}\rangle$. Let $A_1 = \{a, a^6, ab, a^2b, a^5b\}$ when $n = 9$. Then

$$A_1^2 = \{a^2, a^7, a^2b, a^3b, a^6b, a^3, a^7b, a^8b, b, a^4b, 1, a^8, a^5, ab, a^5b, a, a^6, a^4\}.$$

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Let $A_2 = \{a, a^2, a^4, a^5x, a^6x\}$ when $n \geq 10$. Then

$$A_2^2 = \{a^2, a^3, a^5, a^6x, a^7x, a^4, a^6, a^8x, a^8, a^9x, a^{10}x, a^4x, a^3x, ax, 1, a^{-1}, a^5x, a^2x, a\}.$$

It is easy to see that the 18 elements in A_1 are distinct, and the 19 elements in A_2 are distinct. Therefore $|A_1^2| = 18$ and $|A_2^2| = 19$, and then D_{2n} is not a $B(5, 17)$ group. □

THEOREM 2.9. *There is no nontrivial nonabelian $B(5, 17)$ non-2-group.*

PROOF. Let G be a nontrivial nonabelian $B(5, 17)$ non-2-group. It follows from Theorem 2.7 that $G = TP$ where T is a nontrivial normal abelian subgroup of odd order and P is a nontrivial abelian 2-group. Moreover, P has a subgroup Q of index 2 such that Q centralizes T, and each element $x \in P - Q$ inverts both T and Q. Let n be the exponent of T. Since T is abelian, there exists an element $a \in T$ such that $o(a) = n$. We divide the proof into two cases according to whether $|P| = 2$ or $|P| \geq 4$.

Case 1: $|P| = 2$. Let $P = \langle x \rangle$. If $n \geq 9$, then $\langle a, x \rangle = D_{2n}$. It follows from Lemma 2.8 that D_{2n} is not a $B(5, 17)$ group, so neither is G, giving a contradiction.

Thus $n = 3, 5, 7$. Since $|G| \geq 18$ and $|P| = 2$, $|T| \geq 9$. Since T is an abelian group of exponent of 3, 5, 7, it has a subgroup $H = \langle a \rangle \times \langle b \rangle = C_n \times C_n$. Recall that $a^x = a^{-1}$, $b^x = b^{-1}$ and $o(a) = o(b) \geq 3$. Let $A = \{a, ax, abx, b^2x, 1\}$. Then

$$A^2 = \{a^2, a, 1, b^{-1}, ab^{-2}, b, ab^{-1}, a^{-1}b^2, a^{-1}b, a^2x, a^2bx, ab^2x, x, ax, bx, abx, a^{-1}b^2x, b^2x\}.$$

Since subset T and Tx are disjoint, it is easy to check that the 18 elements in A^2 are distinct, and thus G is not a $B(5, 17)$ group, giving a contradiction.

Case 2: $|P| \geq 4$. We first assume that $n \geq 5$. Let $t = ay$ where $y \in Q - \{1\}$. Then $o(t) = 2n \geq 10$. Since the elementary abelian 2-group Q has index 2 in P, the exponent of P is at most 4. If there exists $x \in P - Q$ such that $o(x) = 2$, then the subgroup $\langle t, x \rangle = D_{2m}$ (with $2m = 4n \geq 20$). Thus $\langle t, x \rangle$ is not a $B(5, 17)$ group by Lemma 2.8, so neither is G, giving a contradiction.

Thus we must have $o(x) = 4$ for all $x \in P - Q$. If $o(a) \geq 5$, let $A = \{a, x, a^4x, ax^2, ax^3\}$. Then A^2 contains a subset

$$B = \{a^2, ax, a^2x^2, a^2x^3, a^{-1}x, x^2, a^{-4}x^2, a^{-1}x^3, a^{-1}, a^3x, a^4x^2, a^3x^3, a^3, ax^3, a^2x, x^3, a, x\}.$$

Since P, $aP \cup a^{-4}P$, a^2P, a^3P and $a^4P \cup a^{-1}P$ are disjoint, it is easy to see that the 18 elements in B are distinct, which is a contradiction.

Next assume that $o(a) = 3$. We first consider $|P| = 4$. Then $|T| \geq 5$. Thus T has a subgroup $H = \langle a \rangle \times \langle b \rangle = C_3 \times C_3$. Let $A = \{a, ax, abx, b^2x, b\}$, where $x \in P - Q$. Then

$$A^2 = \{a^2, b^2, ab, b^2x^2, abx^2, bx^2, x^2, ab^2x^2, a^2b^2x^2, a^2bx^2, a^2x, a^2bx, ab^2x, x, ax, bx, abx, a^2b^2x\}.$$

As before, it is easy to show that $|A^2| = 18$, and so G is not a $B(5, 17)$ group, giving a contradiction.

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Thus $|P| > 4$. Then $|Q| \geq 4$. So there exist $y, z \in Q - \{1\}$ such that $x^2 \neq y$ and $x^2 \neq z$. Let $A = \{a, x, a^2y, azx, xz\}$. Then

$$A^2 = \{a^2, y, x^2, a^2zx^2, a, azx^2, ax^2, a^2x^2, ax, a^2zx, a^2x, ayx, a^2yx, yzx, zx, a^2yzx, axz, axyz\}.$$

It is not hard to show $|A^2| = 18$, and so G is not a $B(5, 17)$ group, giving a contradiction.

In each case, we have found a contradiction. Thus, there is no nontrivial nonabelian $B(5, 17)$ group. □

3. The characterization of $B(5, 17)$ 2-groups

We now investigate $B(5, 17)$ 2-groups, and will give a complete characterization of $B(5, 17)$ groups at the end of this section. We first prove some preliminary results.

Lemma 3.1. *Let G be a nonabelian $B(5, 17)$ 2-group such that every proper subgroup of G is abelian. Then G is a trivial $B(5, 17)$ 2-group.*

Proof. Assume that $|G| \geq 32$. Since G is a minimal nonabelian 2-group, it follows from [5, p. 309] that either

$$G = G_1 = \langle a, b \mid a^{2^m} = b^{2^n} = 1, b^{-1}ab = a^{1+2^{m-1}}\rangle, \quad m \geq 2 \text{ and } |G| = 2^{m+n},$$

or

$$G = G_2 = \langle a, b \mid a^{2^m} = b^{2^n} = 1, [a, b]^2 = 1\rangle, \quad m \geq 2 \text{ and } |G| = 2^{m+n+1}.$$

Suppose that $G = G_1 = \{b^ia^j \mid 0 \leq i \leq 2^n - 1, 0 \leq j \leq 2^m - 1\}$. Note that $Z(G) = \langle a^2, b^2\rangle$. We divide the proof into three cases according to whether $m > 3$, $m = 3$ or $m = 2$.

Case 1: $m > 3$. Let $A = \{a, b, ba, ba^2, a^5\}$. Then A^2 contains a subset

$$B = \{b^2, ba, b^2a, a^2, ba^2, ba^3, b^2a^3, b^2a^4, ba^5, a^6, ba^6, ba^7, a^{10}, ba^{1+2^{m-1}}, b^2a^{1+2^{m-1}}, ba^{2+2^{m-1}}, b^2a^{2+2^{m-1}}, ba^{3+2^{m-1}}, b^2a^{3+2^{m-1}}\}.$$

It is easy to show that the 19 elements in B are distinct. Therefore $|A^2| \geq 19$, giving a contradiction.

Case 2: $m = 3$. Recall that $|G| \geq 32$. We know that $n \geq 2$. Let $A = \{a, b, ba, ba^2, b^2\}$. Then

$$A^2 = \{a^2, ba^5, ba^6, ba^7, b^2a, ba, b^2, b^2a^2, b^3, ba^2, b^2a^5, b^2a^6, b^2a^7, b^3a, ba^3, b^2a^3, b^2a^4, b^3a^2, b^4\}.$$

It is easy to show that the 19 elements in A^2 are distinct, giving a contradiction.

Case 3: $m = 2$. As before, we know that $n \geq 3$. Let $A = \{a, b, ab^2, ab^3, ab^5\}$. Then

$$A^2 = \{a^2, ba^3, b^2a^2, b^3a^2, b^5a^2, ba, b^2, b^3a, b^4a^3, b^6a^3, b^3a^3, b^4a^2, b^7a^2, b^3, b^4a, b^5, b^6, b^8, b^6a, b^7, b^{10}\}.$$

It is not hard to show that the first 20 elements in A^2 are distinct, giving a contradiction.

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Next consider $G = G_2$. Let $c = [a, b]$. Since $\langle a, b^2\rangle$ is a proper subgroup of G, it is abelian and thus $[a, b^2] = 1$. Since $cc^b = [a, b][a, b]^b = [a, b^2] = 1$ and $c^2 = 1$, we obtain $c = c^b$. Similarly, we have $c = c^a$. Thus $c \in Z(G)$. Since $ba = abc$, each element of G can be written uniquely as $a^i b^j c^k$, where $0 \le i \le 2^m - 1$, $0 \le j \le 2^n - 1$ and $0 \le k \le 1$.

We divide the proof into two cases according to whether $m > 2$ or $m = 2$.

Case 1: $m > 2$. Let $A = \{a, b, ab, a^3b, a^4\}$. Then

$$A^2 = \{a^2, a^5, a^8, ab, a^2b, a^4b, a^5b, a^7b, b^2, ab^2, a^3b^2, abc, a^2bc, ab^2c, a^4bc, a^2b^2c, a^3b^2c, a^4b^2c, a^6b^2c\}.$$

It is easy to see that the 19 elements in A^2 are distinct. Thus $|A^2| = 19$, giving a contradiction.

Case 2: $m = 2$. Let $A = \{a, b, ab, a^3b, b^3\}$. Then

$$A^2 = \{a^2, b, ab, a^2b, b^2, ab^2, a^3b^2, ab^3, b^4, ab^4, a^3b^4, bc, abc, a^2bc, b^2c, ab^2c, a^2b^2c, a^3b^2c, ab^3c, ab^4c, a^3b^4c\}.$$

It is easy to see that the 21 elements in A^2 are distinct, giving a contradiction.

Thus G is a trivial nonabelian 2-group. □

Lemma 3.2. *If G is a group of order 32 with a maximal subgroup $M \cong Q_8 \times C_2 = \langle a, b, c \mid a^4 = c^2 = 1, a^2 = b^2, ac = ca, bc = cb, a^b = a^3\rangle$, then G is not a $B(5, 17)$ group.*

Proof. Let $A = \{a, b, ab, abc\} \subseteq M$, $B = \{a, b, ab, abc, d\} = \{A, d\}$, where $d \in G - M$. By replacing d by ad, bd or abd if necessary, we can assume that $da \ne ad$ and $db \ne bd$. Let $dA = \{da, db, dab, dabc\}$ and $Ad = \{ad, bd, abd, abcd\}$. It is easy to show that $|A^2| = 12$, and so $|B^2| \ge |A^2 \cup Ad| = 16$.

Replacing a by a^3 if necessary, we can always assume that $db \notin Ad$. If $da \notin Ad$ or $dab \notin Ad$, then $|B^2| \ge |A^2 \cup Ad \cup \{da, db, dab\}| \ge 18$. So we may assume that both $da \in Ad$ and $dab \in Ad$. We divide the proof into the following three cases.

Case 1: $da = abcd$. Then $dab \in Ad - \{abcd\}$, and therefore $dabd^{-1} \in Q_8$. Since $a^{d^{-2}} = (ab)^{d^{-1}} c^{d^{-1}}$, we have $c^{d^{-1}} \in Q_8$. Therefore $c^{d^{-1}} = a^2$, implying that $c = a^2$ since $a^2 \in Z(G)$, giving a contradiction.

Case 2: $da = bd$. Since $dab \in Ad$, we have $dab = ad$, abd, or $abcd$.

(2.1) If $dab = ad$, we know that $db = b^{-1}dab = b^{-1}ad = abd$. Therefore $a = b^d = (ab)^{d^2} = ab$ or a^3b since $d^2 \in Q_8 \times C_2$, giving a contradiction.

(2.2) If $dab = abd$, we assume that $dabc \in Ad$. Then $dabc = ad$ or $abcd$. If $dabc = ad$, we have $abdc = ad$, and so $dcd^{-1} = b^3$, giving a contradiction (because $o(dcd^{-1}) = 2$, but $o(b^3) = 4$). If $dabc = abcd$, we have $abdc = abcd$, and so $dc = cd$. Consider $A_1 = \{a, b, ab, ac\}$. It is easy to show that

$$|A_1^2| = |\{a^2, ab, a^2b, a^2c, a^3b, a, a^3bc, b, ab^2, bc, abc, a^2bc\}| = 12.$$

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Note that

$$A_1 d = \{\underline{ad}, \underline{bd}, \underline{abd}, \underline{acd}\} \quad \text{and} \quad dA_1 = \{da, db, dab, dac\} = \{bd, \underline{a^3 d}, abd, \underline{bcd}\}.$$

It is easy to show that the six underlined elements in $A_1 d \cup dA_1$ are distinct. Let $B = \{A_1, d\}$. Then $|B^2| \geq |A_1^2 \cup A_1 d \cup dA_1| \geq 18$.

(2.3) If $dab = abcd$, we know that $db = b^{-1}dab = b^{-1}abcd = a^3cd$. Therefore $a = b^d = (a^3c)^{d^2} = a^3c$ or ac, giving a contradiction.

Case 3: $da = abd$. Since $dab \in Ad$, we have $dab = ad$, bd, or $abcd$.

(3.1) If $dab = ad$, we assume that $dabc \in Ad$. Then $dabc = bd$ or $abcd$. If $dabc = bd$, we have $adc = bd$, and then $dcd^{-1} = a^3b$, giving a contradiction (because $o(dcd^{-1}) = 2$, but $o(a^3b) = 4$). If $dabc = abcd$, we have $adc = abcd$, and then $dcd^{-1} = bc$. Note that $o(dcd^{-1}) = 2$ and $o(bc) = 4$, so the above gives a contradiction. Therefore $dabc \notin Ad$, and thus $|A^2 \cup Ad \cup dA| \geq 18$.

(3.2) If $dab = bd$, we assume that $dabc \in Ad$. Then $dabc = ad$ or $abcd$. If $dabc = ad$, we have $bdc = ad$, and then $dcd^{-1} = b^3a$. Note that $o(dcd^{-1}) = 2$ and $o(b^3a) = 4$, so the above gives a contradiction. If $dabc = abcd$, we have $bdc = abcd$, and then $dcd^{-1} = b^{-1}abc$, giving a contradiction (for $o(dcd^{-1}) = 2$, but $o(b^{-1}abc) = 4$). Therefore $dabc \notin Ad$, and thus $|A^2 \cup Ad \cup dA| \geq 18$.

(3.3) If $dab = abcd$, we assume that $dabc \in Ad$. Then $dabc = ad$ or bd. If $dabc = ad$, we have $abcdc = ad$, and then $dcd^{-1} = b^3c$, giving a contradiction. If $dabc = bd$, we have $abcdc = bd$, and then $dcd^{-1} = ac$. Note that $o(dcd^{-1}) = 2$ and $o(ac) = 4$, so the above gives a contradiction. Therefore $dabc \notin Ad$, and thus $|A^2 \cup Ad \cup dA| \geq 18$.

In each of the above cases, we have shown that $|B^2| \geq 18$ for some subset B of five elements of G. Therefore G is not a $B(5, 17)$ group. □

Lemma 3.3. *If G is a group of order 32 with a maximal subgroup $M \cong Q_{16} = \langle a, b \mid a^8 = 1, a^4 = b^2, a^b = a^{-1}\rangle$, then G is not a $B(5, 17)$ group.*

Proof. Let $A = \{a, b, ba^3, ba^7\}$ and $B = \{a, b, ba^3, ba^7, c\} = \{A, c\}$, where $c \in G - M$. As before, we may assume that $ac \neq ca$. It is easy to see that

$$|A^2| = |\{a^2, ba^7, ba^2, ba^6, ba, a^4, a^7, a^3, ba^4, a, 1, b, a^5\}| = 13.$$

Note that $Ac = \{ac, bc, ba^3c, ba^7c\}$ and $cA = \{ca, cb, cba^3, cba^7\}$. Since $o(cac^{-1}) = 8$ and $o(b) = o(ba^3) = o(ba^7) = 4$, we conclude that $ca \notin Ac$, so $|B^2| \geq |A^2 \cup Ac \cup ca| = |A^2| + |Ac| + |ca| = 18$. Therefore G is not a $B(5, 17)$ group. □

Lemma 3.4. *If G is a group of order 32 with a maximal subgroup $M \cong P = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3\rangle$, then G is not a $B(5, 17)$ group.*

Proof. Let $A = \{a, b, ba, b^2a\}$ and $B = \{a, b, ba, b^2a, c\} = \{A, c\}$, where $c \in G - M$. It is easy to see that

$$|A^2| = |\{a^2, ba^3, b, b^2a^2, ba, b^2, b^2a, b^3a, ba^2, b^2a^3, b^3a^2, b^3a^3, b^3\}| = 13.$$

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Thus $|B^2| \geq |A^2 \cup Ac| = |A^2| + |Ac| = 17$. Note that $Ac = \{ac, bc, bac, b^2ac\}$ and $cA = \{ca, cb, cba, cb^2a\}$. We can always assume that $ac \neq ca$ and $bc \neq cb$. We may also assume $ca \in Ac$ and $cb \in Ac$, otherwise $|B^2| \geq 18$.

Case 1: $ca = bc$. Then:

(1.1) if $cb = ac$, then $cba = aca = abc = ba^3c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$;

(1.2) if $cb = bac$, then $cba = baca = babc = b^2a^3c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$;

(1.3) if $cb = b^2ac$, then $cba = b^2aca = b^3a^3c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$.

Case 2: $ca = bac$. Then:

(2.1) if $cb = ac$, then $cba = aca = abac = bc$, and thus $cb^2a = acba = abc = ba^3c \notin Ac$, so $|B^2| \geq 18$;

(2.2) if $cb = b^2ac$, then $cba = b^2aca = b^2abac = b^3c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$.

Case 3: $ca = b^2ac$. Then:

(3.1) if $cb = ac$, then $cba = aca = ab^2ac = b^2a^2c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$;

(3.2) if $cb = bac$, then $cba = baca = bab^2ac = b^3a^2c \notin Ac$, which is an 18th distinct element in B^2, so $|B^2| \geq 18$.

In all cases, we have shown that $|B^2| \geq 18$. Thus G is not a $B(5, 17)$ group. □

Lemma 3.5. *If G is a group of order 32 with a maximal subgroup $M \cong D = \langle a, b, c \mid a^2 = b^2 = c^4 = 1, ac = ca, bc = cb, a^b = c^2a\rangle$, then G is not a $B(5, 17)$ group.*

Proof. Let $A = \{a, b, ab, bc\}$ and $B = \{a, b, ab, bc, d\} = \{A, d\}$, where $d \in G - M$. It is easy to see that

$$|A^2| = |\{1, a, b, c, ac, ac^2, ac^3, ba, bac, bac^2, bac^3, bc^2, c^2\}| = 13.$$

Thus $|B^2| \geq |A^2 \cup Ad| = |A^2| + |Ad| = 17$. Note that $Ad = \{ad, bd, abd, bcd\}$ and $dA = \{da, db, dab, dbc\}$. As before, we assume that $da \neq ad$ and $db \neq bd$. Next we assume that $da, db \in Ad$. Since $o(a) = 2$, but $o(ab) = o(bc) = 4$, we must have $da = bd$. Similarly, since $o(b) = 2$, we have $db = ad$. Then $dab = bdb = bad \notin Ad$, which is an 18th distinct element in B^2. Therefore $|B^2| \geq 18$, and G is not a $B(5, 17)$ group. □

Lemma 3.6. *If G is a group of order 32 with a maximal subgroup $M \cong D_8 \times C_2 = \langle a, b, c \mid a^4 = b^2 = c^2 = 1, ac = ca, bc = cb, a^b = a^3\rangle$, then G is not a $B(5, 17)$ group.*

Proof. Let $A = \{a, b, ba^3, ba^3c\}$ and $B = \{a, b, ba^3, ba^3c, d\} = \{A, d\}$, where $d \in G - M$. We can always assume that $da \neq ad$. It is easy to see that

$$|A^2| = |\{a^2, ba^3, ba^2, ba^2c, ba, 1, a^3, a^3c, b, a, c, bc, ac\}| = 13.$$

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

Note that $Ad = \{ad, bd, ba^3d, ba^3cd\}$ and $dA = \{da, db, dba^3, dba^3c\}$. Since $o(dad^{-1}) = 4$ and $o(b) = o(ba^3) = o(ba^3c) = 2$, we conclude that $da \notin Ad$. Thus $|B^2| \geq |A^2 \cup Ad \cup da| = |A^2| + |Ad| + |da| = 18$. Therefore G is not a $B(5, 17)$ group. □

We are now ready to prove the main result of this section.

Theorem 3.7. *There is no nontrivial nonabelian* $B(5, 17)$ 2-*group.*

Proof. The proof is by the minimal counterexample method. Suppose on the contrary that there is a nontrivial nonabelian $B(5, 17)$ 2-group G with minimal order. Then either every proper subgroup of G is abelian or $|G| = 32$.

Suppose that $|G| = 32$. We claim that every maximal subgroup M of G is a $B(4, 13)$ group. Otherwise, there exists a subset $A = \{a, b, c, d\} \subseteq M$ such that $|A^2| \geq 14$. Let $S = \{a, b, c, d, e\}$ where $e \in G - A$. Then $S^2 \supseteq A^2 \cup \{ae, be, ce, de\}$, and therefore $|S^2| \geq |A^2| + 4 \geq 18$, which implies that G is not a $B(5, 17)$ group, giving a contradiction. Next we prove that every proper subgroup of G is abelian. Assume that there exists a nonabelian maximal subgroup M of G. Then M is a $B(4, 13)$ group of order 16. By [7, Lemma 2.23], M must be one of the following groups: $Q_8 \times C_2$, Q_{16}, P, D or $D_8 \times C_2$. However, by Lemmas 3.2, 3.3, 3.4, 3.5 and 3.6, we know that none of these cases is possible.

Therefore every proper subgroup of G is abelian. By Lemma 3.1, G is a trivial $B(5, 17)$ group, giving a contradiction. □

Combining Theorems 2.9 and 3.7, we obtain a complete characterization of $B(5, 17)$ groups.

Theorem 3.8. *A group* G *is a* $B(5, 17)$ *group if and only if* G *is either abelian or a nonabelian trivial* $B(5, 17)$ *group.*

4. On $B(5, 15)$ and $B(5, 16)$ groups

Using the complete characterization of $B(5, 17)$ groups given in the previous section, we can easily characterize $B(5, 15)$ and $B(5, 16)$ groups.

We first investigate $B(5, 16)$ groups and assume that G is a nontrivial nonabelian $B(5, 16)$ group. Then $|G| \geq 18$. Since $|G|$ is also a nontrivial nonabelian $B(5, 17)$ group, by Theorem 3.8, no such group exists. We state this result as follows.

Theorem 4.1. *A group* G *is a* $B(5, 16)$ *group if and only if either* G *is abelian or* G *is a nonabelian trivial* $B(5, 16)$ *group.*

We next consider $B(5, 15)$ groups and provide a short proof for the main result in [6] which gives a complete characterization of $B(5, 15)$ groups.

Theorem 4.2. *A group* G *is a nontrivial nonabelian* $B(5, 15)$ *group if and only if* $G \cong Q_8 \times C_2$.

Proof. Let G be a nontrivial nonabelian $B(5, 15)$ group. We first assume that G is not a 2-group. Then $|G| \geq 18$. Thus, G is a nontrivial nonabelian $B(5, 17)$ group.

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press

By Theorem 2.9, no such group exists. Next we assume that G is a 2-group. Since G is a nonabelian $B(5, 17)$ group, it follows from Theorem 3.8 that $|G| = 16$. It was proved in [10] that $Q_8 \times C_2$ is a $B(5, 15)$ group of order 16. In addition to this group, there are eight non-abelian 2-groups of order 16. A direct calculation shows that for each such group G, there exists a subset S of five elements of G such that $|S^2| = 16$, and thus G is not a $B(5, 15)$ group (see [2] for the detailed calculation). Therefore $G \cong Q_8 \times C_2$ is the only nontrivial nonabelian $B(5, 15)$ group. □

References

[1] Y. G. Berkovich, G. A. Freiman and C. E. Praeger, 'Small squaring and cubing properties for finite groups', *Bull. Aust. Math. Soc.* **44** (1991), 429–450.

[2] T. Eddy, 'Classifying groups with small squaring properties', Master's Thesis, Memorial University of Newfoundland, St. John's, Newfoundland, Canada, 2006.

[3] T. Eddy and M. M. Parmenter, 'Groups with restricted squaring properties', *Ars Combin.*, accepted.

[4] G. A. Freiman, 'On two- and three-element subsets of groups', *Aequationes Math.* **22** (1981), 140–152.

[5] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

[6] Y. Li and Y. Tan, 'On B_5-groups', *Ars Combin.*, accepted.

[7] Y. Li and Y. Tan, 'On $B(4, 13)$ 2-groups', *Comm. Algebra.*, accepted.

[8] Y. Li and Y. Tan, 'On $B(4, k)$ groups', *J. Algebra Appl.* **9** (2010), 27–42.

[9] P. Longobardi and M. Maj, 'The classification of groups with the small squaring property on 3-sets', *Bull. Aust. Math. Soc.* **46** (1992), 263–269.

[10] M. M. Parmenter, 'On groups with redundancy in multiplication', *Ars Combin.* **63** (2002), 119–127.

[11] D. J. S. Robinson, *A Course in the Theory of Groups* (Springer, Berlin–Heidelberg–New York, 1982).

YUANLIN LI, Department of Mathematics, Brock University, St. Catharines, Ontario, Canada L2S 3A1
e-mail: yli@brocku.ca

XIAOYING PAN, Department of Mathematics, Brock University, St. Catharines, Ontario, Canada L2S 3A1
e-mail: kp09vn@brocku.ca

https://doi.org/10.1017/S0004972711002474 Published online by Cambridge University Press