Groups With Restricted Squaring Properties

Terry Eddy[1] and M.M. Parmenter[2]

1. INTRODUCTION

For a subset S of a finite group G we set $S^2 = \{xy|x, y \in S\}$. If, for some positive integer n, G has the property that $|S| = n$ implies $|S^2| < n^2$ then G is said to have the small squaring property on n-sets. Groups with this property have been characterized by Freiman [2] when $n = 2$, and by Berkovich, Freiman, Praeger[1] and Longobardi, Maj[3] when $n = 3$.

For G abelian, $|S| = n$ implies $|S^2| \leq \frac{n(n+1)}{2}$ and, in general, groups with this property are called B_n-groups. B_2-groups were characterized in [2](as noted above), while B_3-groups and B_4-groups were characterized in [4].

The following definition generalizes both the above notions.

1.1 Definition

Let n, k be positive integers with $k \leq n^2 - 1$. A group G is called a $B(n, k)$ group if $|\{a_i a_j | 1 \leq i, j \leq n\}| \leq k$, for any n-subset $S = \{a_1, ... a_n\}$ of G.

So B_n-groups are $B(n, \frac{n(n+1)}{2})$ groups, while groups with the small squaring property on n-sets are $B(n, n^2 - 1)$ groups.

In this paper we complete the classification of $B(2, k)$ groups and $B(3, k)$ groups for all values of k. These results are presented in the next section. All but the $B(3, 7)$ case are quite straightforward, and the proof of this latter case is left to Section 3.

It is assumed throughout that all groups are finite (though some arguments do extend to the infinite case).

2. RESULTS

We begin with the previously mentioned result of Freiman[2]. A proof is included for convenience.

Theorem 2.1 A group G is $B(2, 3)$ if and only if G is either abelian or a Hamiltonian 2-group.

[1] A substantial part of this paper is from the first author's M.Sc. thesis.

[2] The second author's research was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

Proof: $\Longleftarrow$

We take a subset $\{x, y\}$ where $x, y \in G$. If G is abelian, we have $xy = yx$, and thus there exist at most three distinct products. So we check the case where G is a Hamiltonian 2-group, i.e. $Q_8 \times C_2 \ldots \times C_2$ where Q_8 is the quaternion group of order 8. We may assume by the last remark that x and y do not commute. But since all elements of order 2 are central, then $x^2 = y^2$, and so there exist at most three distinct products. Consequently, the listed groups are $B(2,3)$.

$\Longrightarrow$

Assume G is a nonabelian $B(2,3)$ group. Consider the subset $\{x, y\}$, where $x, y \in G$ do not commute. Since G is a $B(2,3)$ group, this forces $x^2 = y^2$. Next, we consider the subset $\{x, xy\}$. Again, x and xy don't commute, so we get $x^2 = (xy)^2 = xyxy \Rightarrow x = yxy$ or $y^{-1}xy = xy^2 \Rightarrow y^{-1}xy = x^3$ since $y^2 = x^2$. So G is Hamiltonian, or equivalently, $G \cong Q_8 \times C_2 \times \ldots \times C_2 \times A$ where A is abelian and $|A|$ is odd.

Note that $\{x, y^3\} = \{x, x^2y\}$. Since x and x^2y don't commute, $x^2 = (y^3)^2 = y^6 = x^6$, so $x^4 = 1$ for all noncentral $x \in G$. It follows that $|A| = 1$ and we're done. □

Next we classify B(2,2) groups.

Proposition 2.2 A group G is a $B(2,2)$ group if and only if G is an elementary abelian 2-group.

Proof: $\Longleftarrow$

Consider a subset $\{x, y\}$ where $x, y \in G$, from which we get the products x^2, xy, yx, y^2. Clearly, $yx = xy$ and $x^2 = 1 = y^2$, so we can obtain only two distinct products. Therefore G is $B(2,2)$.

$\Longrightarrow$

Let G be a $B(2,2)$ group. If we consider the subset $\{1, x\}$, we obtain the products $1, x, x^2$, of which only two are distinct, hence, by the cancelation law, we must have $x^2 = 1$. It follows that every element of G must be of order 2. Consequently G is abelian and hence $G \cong C_2 \times \ldots \times C_2$, as required. □

This completes the classification of $B(2,k)$ groups for all positive integers k. It is convenient to begin the study of $B(3,k)$ groups with the case $k = 6$.

Theorem 2.3[4] A group G is a $B(3,6)$ group if and only if either $|G| \leq 6$ or G is abelian.

Next we observe that if $G \cong S_3 =< a, b | a^3 = b^2 = 1, ba = a^2b >$, then the subset $S = \{a, b, ab\}$ satisfies $|S^2| = 6$. Hence S_3 is not a $B(3,k)$ group when $k \leq 5$, and it follows from Theorem 2.3 that when studying such groups we may assume G is abelian.

Proposition 2.4 A group G is a $B(3,3)$ group if and only if $|G| \leq 3$.
Proof:

Assume G is a $B(3,3)$ group. Taking a subset $\{1, x, y\}$, we get the products $1, x, y, x^2, xy, y^2$. Since only three of these are distinct, the products x^2, xy, y^2 must be equal to either 1, x or y. Using the cancellation law, we get $xy = 1$, and we are left with the possibilities $x^2 = 1$ or $x^2 = y$. But in the first case $x^2 = 1 = xy$ from above, contradicting the cancellation law, so $x^2 = y$. This means that G can have only three elements. □

Proposition 2.5 A group G is a $B(3,4)$ group if and only if either $|G| \leq 4$ or G an elementary abelian 2-group.
Proof: $\Longleftarrow$

If $G \cong C_2 \times \ldots \times C_2$, take any subset $\{x, y, z\}$. Since $x^2 = y^2 = z^2 = 1$, G is $B(3,4)$.

$\Longrightarrow$

Assume G is a $B(3,4)$ group and x is of order greater than 2. Taking the subset $\{1, x, x^2\}$, we get the products $1, x, x^2, x^3, x^4$. Since these products cannot be distinct, x must be of order ≤ 4.

Now, if $|G| > 4$ then G must also contain an element y such that y is not in $\langle x \rangle$. If we consider the subset $\{1, x, y\}$, we get the products 1, x, y, x^2, xy, y^2. However, 1, x, y, x^2, and xy are all distinct, which is a contradiction. Therefore no such x exists, and $G \cong C_2 \times \ldots \times C_2$ as desired.
□

Proposition 2.6 A group G is a $B(3,5)$ group if and only if G satisfies one of the following:

(i) $|G| \leq 5$

(ii) G is an elementary abelian 2-group.

(iii) $G \cong C_4 \times E$ where E is an elementary abelian 2-group.

(iv) $G \cong C_6$

Proof: $\Longleftarrow$

If $G \cong C_6 = \langle x \rangle$, we consider a subset $\{x^a, x^b, x^c\}$. Multiplying, we get the products $x^{2a}, x^{a+b}, x^{a+c}, x^{2b}, x^{b+c}, x^{2c}$, whereby the sum of these exponents is $4a + 4b + 4c$. However, the sum of the exponents of the set $x^0, x^1, x^2, x^3, x^4, x^5$ is 15, but since $4a + 4b + 4c \not\equiv 15 (mod\ 6)$, our list of products cannot produce all powers of x. Therefore we have at most five distinct powers of x present, so C_6 is $B(3,5)$ as required.

If $G \cong C_4 \times C_2 \times \ldots \times C_2$ we know that either $x^2 = 1$ or x^2 is the element $(a^2, 1, \ldots, 1)$ of order 2. So if we take a subset $\{x, y, z\}$, then two of x^2, y^2, z^2 must be equal, and consequently, $G \cong C_4 \times C_2 \times \ldots \times C_2$ is $B(3,5)$.

$\Longrightarrow$

We next assume that G is $B(3,5)$. If we can choose x of order greater than 3, consider the subset $S = \{1, x, x^3\}$. Then, multiplying in the usual way, we get the products $1, x, x^3, x^2, x^4, x^6$. These elements cannot all be distinct, so we have proved that every element has order at most 6. It is necessary, therefore, to consider only the groups $C_4 \times \ldots \times C_4 \times C_2 \times \ldots \times C_2, C_3 \times \ldots \times C_3 \times C_2 \times \ldots \times C_2$ (with perhaps no C_2 terms in these cases)and $C_5 \times \ldots \times C_5$.

Assume first that we can take the subset $\{x, y, xy\}$, where x, y are generators of different C_k's, with $k > 2$. From here we get the products x^2, xy, x^2y, y^2,
xy^2, x^2y^2 which are all distinct, and so we cannot have more than one such C_k. We are left with the possibility that either $G \cong C_4 \times C_2 \times \ldots \times C_2$ or $G \cong C_3 \times C_2 \times \ldots \times C_2$, with at least one C_2 term. To finish we must investigate the latter.

Consider the subset $\{1, xy, x^2z\}$ where $x \in C_3$ and y, z are generators of different C_2's. Since the products $1, xy, x^2z, x^2, yz, x$ are clearly all distinct, we have a contradiction. Therefore we can have only $C_3 \times C_2 \cong C_6$ and we're done. □

Here is the result classifying $B(3,7)$ groups. As mentioned in the introduction, the next section will be devoted to its proof.

Theorem 2.7 A group G is a $B(3,7)$ group if and only if G satisfies one of the following:

(i) G is abelian

(ii) $G \cong S_3$

(iii) $G = \langle a, p | a^6 = 1, a^3 = p^2, pa = a^5p \rangle$

(iv) G is a Hamiltonian 2 - group.

3. PROOF OF THEOREM 2.7

We will start by showing that the groups listed are $B(3,7)$ groups. Cases (i) and (ii) are obvious.

Lemma 3.1 $G = \langle a, p | a^6 = 1, a^3 = p^2, pa = a^5p \rangle$ is a $B(3,7)$ group.

Proof

We note first that $A = \langle a \rangle$ is a cyclic subgroup of G, and the set of elements $H = \{p, ap, \ldots, a^5p\}$ all have the same square, namely a^3. We also see that in this group there are six elements of order 4 (the set H), two elements each of orders 3 and 6, one element of order 2, and the identity. We proceed by taking a subset $\{x, y, z\}$ and investigating the different possibilities of the orders of x, y and z in an effort to find at least two repetitions of products in each case. Note that if any of x, y, z are of order at most 2, then such an element would be central and would automatically give two repetitions. So we assume that each of x, y, z are of order at least 3 and consider the following cases.

(i) $|x| = 3$, $|y| = 6$, $|z| = 3$ or $|x| = 3$, $|y| = 6$, $|z| = 6$

Since all of these elements are contained in the cyclic subgroup A mentioned above, x, y, z will commute with each other, immediately giving at least 2 repetitions.

(ii) $|x| = 3$, $|y| = 4$, $|z| = 6$

This is the subset $\{a^i, a^j, a^k p\}$ where $i = 1$ or 5, $j = 2$ or 4, $0 \leq k \leq 5$, which gives the products $a^{2i}, a^{i+j}, a^{i+k}p, a^{i+j}, a^{2j}, a^{j+k}p, a^{k-i}p, a^{k-j}p, a^3$. We already have the product a^{i+j} repeated once, so we need only find one more repetition. We examine all possible values of i and j.

i	j	resulting repetition
1	2	$a^3 = a^{i+j}$
1	4	$a^{2i} = a^{2j}$
5	2	$a^{2i} = a^{2j}$
5	4	$a^{i+j} = a^3$

We have found a repetition for all possible values of i and j, so we have the required two repetitions for this case.

(iii) $|x| = 3$, $|y| = 3$, $|z| = 4$

This is the subset $\{a^2, a^4, a^i p\}$ where $0 \leq i \leq 5$, which gives the products $a^4, 1, a^{i+2}p, 1, a^2, a^{i+4}p, a^{i+4}p, a^{i+2}p, a^3$. Clearly 1, $a^{i+4}p$ and $a^{i+2}p$ appear twice, so this case holds.

(iv) $|x| = 6$, $|y| = 6$, $|z| = 4$

This is the subset $\{a, a^5, a^i p\}$ where $0 \leq i \leq 5$, which gives the products $a^2, 1, a^{i+1}p, 1, a^4, a^{i+5}p, a^{i+5}p, a^{i+1}p, a^3$. Clearly 1, $a^{i+5}p$ and $a^{i+1}p$ appear twice, so this case holds.

(v) $|x| = 3$, $|y| = 4$, $|z| = 4$ or $|x| = 6$, $|y| = 4$, $|z| = 4$

This is the subset $\{a^i, a^j p, a^k p\}$ where $i = 1, 2, 4, 5$; $0 \leq j \leq 5$, $0 \leq k \leq 5$, which gives the products $a^{2i}, a^{i+j}p, a^{i+k}p, a^{j-i}p, a^3, a^{j-k+3}, a^{k-i}p, a^{k-j+3}$, a^3. We already have the product a^3 repeated once, so we need only find one more repetition.

If $i = 1$, we have the products $a^2, a^{1+j}p, a^{1+k}p, a^{j-1}p, a^{j-k+3}, a^{k-1}p$, a^{k-j+3}, a^3. We now check the differences (mod 6)between j and k using these products.

$k-j$	resulting repetition
1	$a^2 = a^{j-k+3}$
2	$a^{1+j}p = a^{k-1}p$
3	$a^{j-k+3} = a^{k-j+3}$
4	$a^{1+k}p = a^{j-1}p$
5	$a^{k-j+3} = a^2$

Hence, we get the necessary repetition for all values of j and k when $i = 1$. A similar calculation shows that $i = 2, 4$ and 5 also yield another repetition completing the proof of this case.

(vi) $|x| = 4$, $|y| = 4$, $|z| = 4$ We know all the order 4 elements in G are of the form $a^i p$ and $(a^i p)^2 = a^3$ for all i, immediately giving the required two repetitions.

We have checked all possible cases, so G is a $B(3,7)$ group, as required. □

Lemma 3.2 If G is a Hamiltonian 2-group then G is a $B(3,7)$ group.

Proof

In such a group all non-central elements have the same square. It follows that if $S = \{x, y, z\}$ where x, y, z are all non-central then $|S^2| \leq 7$. But if x is central then $xy = yx$ and $xz = zx$, again giving $|S^2| \leq 7$. So G is a $B(3,7)$ group. □

The proof of the other direction of Theorem 2.7 is quite lengthy and will proceed using a number of lemmas. For the rest of this section it will be assumed that G is a nonabelian $B(3,7)$ group.

We remark that in order to keep the proof as self-contained as possible we have chosen to include some arguments which were previously seen in [1] (in the case of $B(3,8)$ groups). In addition we will use some of the same notation as was introduced there.

Lemma 3.3 If $x, y \in G$ are of odd order then x and y commute.

Proof:

We assume $yx \neq xy$ and take the subset $\{x, x^{-1}, y\}$ from which we get the products $x^2, 1, xy, x^{-2}, x^{-1}y, yx, yx^{-1}, y^2$. Using our assumptions and the cancellation law, we eliminate many of the possible equalities between products and are left to investigate the following:

(i) $x^2 = y^2 \Rightarrow x^2$ and y^2 commute. But this implies that x and y commute, since $x \in \langle x^2 \rangle$ and $y \in \langle y^2 \rangle$. A similar argument holds for the case when $x^{-2} = y^2$.

(ii) $xy = yx^{-1} \Rightarrow y^{-1}xy = x^{-1} \Rightarrow y^{-2}xy^2 = y^{-1}x^{-1}y \Rightarrow y^{-2}xy^2 = (y^{-1}xy)^{-1}$. So we have $y^{-2}xy^2 = (x^{-1})^{-1} \Rightarrow xy^2 = y^2x$. But $y \in \langle y^2 \rangle$,

therefore x and y^2 cannot commute. A similar argument holds for $x^{-1}y = yx$.

All cases fail, so there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. So x and y commute. □

Lemma 3.4 If $x \in G$ is of odd order and $y \in G$ is of order 2^m for some integer m, then x and y^2 commute.

Proof:

We assume $y^2x \neq xy^2$ and again take the subset $\{x, x^{-1}, y\}$. Similar arguments to those seen in the proof of Lemma 3.3 yield a contradiction. □

Lemma 3.5 If $x \in G$ is of odd order greater than 3 and $y \in G$ is of order 2^m for some integer m, then x and y commute.

Proof:

This time we assume $yx \neq xy$ and take the subset $\{x, x^2, y\}$. Multiplying in the usual way we get the products $x^2, x^3, xy, x^4, x^2y, yx, yx^2, y^2$. Using our assumptions and the cancellation law, as before, we eliminate many of the possible equalities between products and are left to investigate one possibility:

$xy = yx^2 \Rightarrow y^{-1}xy = x^2 \Rightarrow y^{-1}xy = (yx^2y^{-1})^2$ since $x = yx^2y^{-1}$. But then $y^{-1}xy = yx^4y^{-1} \Rightarrow x = y^2x^4y^{-2}$. Applying the last lemma, it is clear that x and y^2 commute giving $x^4 = x \Rightarrow x^3 = 1$. This contradicts our assumption that $|x|$ is greater than 3. The case where $x^2y = yx$ proceeds in the same way.

Since all cases fail, so there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. Therefore, x and y commute. □

Lemma 3.6 If $x, y \in G$ are both of order 3, with $y \neq x$ and $y \neq x^2$, and $z \in G$ is of order 2^m for some integer m, then z commutes with both x and y.

Proof:

We may assume that z does not commute with either x or y (replacing x or y with xy if needed(using Lemma 3.3)). It is clear also that z doesn't commute with x^2 or y^2. Thus if $z^{-1}xz = y$ we replace y with y^2, so we can assume $z^{-1}xz \neq y$. Also, it follows from Lemma 3.4 that $z^{-1}yz \neq z^{-2}xz^2 = x$, so we consider the subset $\{x, y, z\}$ and multiply in the usual way to get the products $x^2, xy, xz, y^2, yz, zx, zy, z^2$.

Using similar arguments to those seen before we find that there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. Therefore, z commutes with both x and y. □

Lemma 3.7 If $x \in G$ is of order $3, y \in G$ is of odd order greater than 3, and $z \in G$ is of order 2^m for some integer m, than z commutes with both x and y.

Proof:

We know from Lemma 3.5 and Lemma 3.3 above that y commutes with z, and x commutes with y. Since $|xy|$ is odd and greater than 3, Lemma 3.5 says that xy commutes with z, and therefore x also commutes with z. □

We will now use the previous lemmas to obtain information on the structure of G when G is a $B(3,7)$ group. Let $T = \{g \in G \mid \text{the order of g is odd}\}$. It follows from Lemma 3.3 that T is an abelian normal subgroup of G. Also if P is a Sylow 2-subgroup of G then $G = TP$.

Lemma 3.8 There are two possibilities for T, either $|T| = 3$ or T is central in G.

Proof:

Assume that $|T| > 3$ and let $x \neq 1$ be any element of T. Let $z \in G$ be such that $|z| = 2^n$ for some n. If $|x| > 3$, then Lemma 3.5 says that x and z commute. On the other hand, if $|x| = 3$ we can choose $y \in T$ such that $y \notin \langle x \rangle$ (since $|T| > 3$). It follows from Lemmas 3.6 and 3.7 that z commutes with both x and y.

So in all cases x and z commute and we conclude from Lemma 3.3 that x is central. Thus T is central. □

Lemma 3.9 If T is central in G then $T = \{1\}$.

Proof:

Assume T is central in G. If P is a Sylow 2-subgroup of G, then P is nilpotent and nonabelian because $G = T \times P$ and T is central in G with G nonabelian. As a consequence it is not difficult to find maximal subgroups $M \neq N$ of P such that there exist $a \epsilon M - N$ and $b \epsilon N - M$ with $ab \neq ba$.

Next, let $t \in T$, $t \neq 1$. If we select $S = \{a, bt, abt^2\}$, where a and b are chosen as above, then S^2 contains the nine products $a^2, abt, a^2bt^2, bat, b^2t^2, babt^3, abat^2, ab^2t^3, ababt^4$. We now try to show that more than seven of these are distinct. If $t^3 \neq 1$ this is straightforward, so we will assume that $t^3 = 1$ from now on. We use the cancellation law with the fact that $ab \neq ba$ to eliminate most of the possibilities and are left to investigate the following:

- If we take $bab = a^2$ then $b^{-1}ab = b^{-2}a^2 \in M \cap N \Rightarrow a = b(b^{-2}a^2)b^{-1} \in M \cap N$. But then this implies that $a \in N$, a contradiction, so bab and a^2 are distinct. A similar argument holds for the case where $b^2t^2 = abat^2$.
- If we let $ababt = bat$ then $a^{-1}ba = bab = b^2(b^{-1}ab) \in M$, which contradicts $b \in N - M$. So these products are distinct.

We are left with more than seven distinct products, hence no such t can be chosen to satisfy the condition that G is $B(3,7)$. Thus $T = \{1\}$ as required. □

Now we will proceed with the proof of Theorem 2.7. Assume first that G is not a 2-group, in which case we have shown that $|G| = 3(2^n)$ for some n, and $G = TP$ where $T =< t >$ is the unique Sylow 3-subgroup of G, T is not central in G and P is a Sylow 2-subgroup of G.

Set $Q = \{x \in P|xt = tx\}$. Since T is not central in G, $P \neq Q$. If $w \in P - Q$ then $wtw^{-1} = t^2$, and it follows that Q is of index 2 in P. We may assume $|G| \geq 8$, so $|P| > 2$ and it follows that $|Q| \geq 2$. We must now check two cases.

Case 1: P is abelian

We choose (if possible) $p \in P - Q$ and $q \neq 1 \in Q$ with $p^2 \neq q$, and let $S = \{pq, tp, tq\}$. Multiplying the elements of S in the usual way, we get the products $p^2q^2, pqtp, pq^2t, tp^2q, tptp, tptq, tpq^2, t^2qp, t^2q^2$. Using the earlier remark that $ptp^{-1} = t^2$, this list can be rewritten as $p^2q^2, p^2qt^2, pq^2t, p^2qt, p^2$, pq, pq^2t^2, pqt, q^2t^2. The cancellation law tells us that the only possibility for equality here is $p^2q^2 = p^2$. So there must be at least eight distinct products, giving a contradiction. It follows then that we must have $p^2 = q$.

We can conclude that $P = \langle p \rangle$ must be cyclic of order 4. Therefore the group in question is exactly $G = \langle p, t | p^4 = 1, t^3 = 1, pt = t^2p \rangle$ of order 12. But it is easy to see that this is isomorphic to the group listed in case (iii) of Theorem 2.7.

Case 2: P is not abelian

Note that $P =< P - Q >$, so there exist $a, c \in P - Q$ such that $ac \neq ca$. Since Q is of index 2 in P it follows that $ac \in Q$ Setting $b = ac$ we have $a \in P - Q$ and $b \in Q$ such that $ab \neq ba$.

Now we choose two particular subsets.

(*i*) First, we choose the subset $S = \{a, b, t\}$, with $t \in T$. Multiplying in the usual way we get the products $a^2, ab, at, ba, b^2, bt, ta, tb, t^2$. Since $bt = tb$, we use our assumptions above and the cancellation law to eliminate all other possible equalities except for $a^2 = b^2$. So we get eight distinct products unless $a^2 = b^2$. Note that we can replace $a \in S$ by $ab \in P - Q$ since $(ab)b \neq b(ab)$, which gives us $abab = b^2$.

(*ii*) We now choose another subset $S = \{a, tb, t\}$. Multiplying the elements of S we get the eight products $a^2, atb, at, tba, t^2b^2, t^2b, ta, t^2$, which can be rewritten as a^2, abt, at, bat^2, b^2t^2, bt^2, at^2, t^2. Clearly, the only possible equality is $b^2t^2 = t^2$, forcing $b^2 = 1$. So we get eight distinct products unless $b^2 = 1$.

So now we have $a^2 = b^2 = abab = 1$ which implies that $aba = b \Rightarrow aba^2 = ba \Rightarrow ab = ba$, contradicting our assumption that $ab \neq ba$. Thus Case 2 cannot possibly exist and so, the proof of Theorem 2.7 is complete in the case where G is not a 2-group.

For the rest of this section we will assume G is a 2-group, and will make use of the classification of $B(3,8)$ groups obtained in [1] and [3]. The following easy result settles the issue.

Proposition 3.10 Let G be a 2-group with an abelian subgroup A of index 2. Assume that $a^x = a^{-1}$ for all $a \in A$ where $x \notin A$. Then if G is a $B(3,7)$ group, G must be abelian or Hamiltonian.

Proof:

Assume G is neither abelian nor Hamiltonian. It follows that there exists $a \in A$ such that $a^2 \neq 1$ and $x^2 \neq a^2$. Consider $\{a, x, ax\}$. The products are $a^2, ax, a^2x, a^{-1}x$,
$x^2, a^{-1}x^2, x, ax^2, x^2$. Note that x^2 is repeated but all other products are distinct (and not equal to x^2), contradicting G being $B(3,7)$. □

Looking at the classification of $B(3,8)$ groups we see that the D-groups and Q-groups mentioned in Theorem 2 of [1] both satisfy the conditions given in Proposition 3.10, as do the groups listed under (3) in Theorem A of [3]. The groups listed under (4) and (5) in Theorem A of [3] have the dihedral group of order 8 as a homomorphic image and thus can't be $B(3,7)$ (again using Proposition 3.10).

This leaves only groups listed under (2) in Theorem A, i.e. groups for which $< x^2 | x \in G >$ is of order 2. So assume G is of this type and let $< x^2 | x \in G >= \{1, z\}$. Note that z is central and $\{1, z\}$ is the commmutator subgroup of G.

Assume for the moment that we can choose $a, b \in G$ which don't commute such that either $a^2 = 1$ or $b^2 = 1$. Consider $\{a, b, ab\}$, which gives the products $a^2, ab, a^2b, abz, b^2, ab^2z, a^2bz, ab^2, a^2b^2z$.

Note that exactly two of $\{a^2, b^2, a^2b^2z\}$ are equal while the other six products are distinct (from each other and from the three just listed), contradicting G being a $B(3,7)$ group.

We are left with the possibility that $a^2 = z$ and $b^2 = z$ whenever $a, b \in G$ don't commute. But in that case $a^{-1}ba = a^{-1}(abz) = bz = b^3$, and so G is Hamiltonian.

The proof of Theorem 2.7 is complete. □

The authors would like to thank the referee for several helpful suggestions.

REFERENCES

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

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

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

[4] Parmenter, M.M., *On groups with redundancy in multiplication*, Ars Combinatoria **63** (2002), 119-127.

Department of Mathematics and Statistics
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
A1C 5S7