Finite groups and their breadth.

Hermann Heineken and Francesco G. Russo

Introduction; notations.

Frobenius conjectured 1895 the following: If n is a divisor of the order $|G|$ of a finite group G, then the number $L_n(G) = |\{x | x \in G;\ x^n = 1\}|$ is divisible by n. This has been proved recently completely by Iiyori and Yamaga 1991.
This has also lead to consider the quotient $n^{-1}L_n(G) = b_n(G)$, which we will call the *(local n-)breadth* of G, and its maximum, namely $Max_{n||G|}(b_n(G)) = B(G)$,the *(global) breadth* of G.
Meng and Shi were the first to consider the groups G satisfying $B(G) = 2$. All of these classes of groups G with $B(G) = n$ consist of infinitely many isomorphism classes, so the reduction to a "nucleus" of (hopefully) finitely many isomorphism classes together with a recipe how to find all further members could be helpful.

A first step in this direction is to look for the *refined* groups:
A group G is refined, if $B(G/N) < B(G)$ for all proper normal subgroups N of G; on the other hand, H is *deduced* (from G) if G is an epimorphic image of H and $B(H) = B(G)$.
So here we have a reduction, and the recipe of deducing will be given below. It is helpful that the structure of the kernel of the epimorphism mentioned before is very restricted, as we will see.

First statements on local and global breadth.

Recall that global breadth is the maximum of local breadths. We obtain

(i) $B(H \times G) = B(H)B(G)$ if $(|H|, |G|) = 1$,

(ii) $B(H) \leq B(G)$ if $H \subseteq G$,

(iii) If $p||G|$ is a prime, then $b_p(G) = k(p-1)+1$ for some integer k.

(Remember for (iii) that $L_p(G)$ is divisible by p and $L_p(G) - 1$ is divisible by $p-1$.)

(iv) If $p||G|$ is a prime and $B(G) < p$, then the Sylow p-subgroup of G is normal and cyclic,

(v) If $p||G|$ is a prime and $2B(G) < p$, then the Sylow p-subgroup of G belongs $Z(G)$.

(Here (v) follows from (iv) and $2B(X) \leq p+1$ for non-abelian subgroups X of $Hol(C_p)$.)

Corollary 1.
If $B(G) = n$, then $G = H \times V$ where V is cyclic and divisible only by primes greater than $2n$ while $|H|$ is divisible only by primes smaller than $2n$ and $B(H) = B(G)$.
The following is a generalization of (iii):
(vi) If $n||G|$ then $L_n(G) - 1$ is divisible by $gcd(p_i - 1)$ of all prime divisors p_i of n.
Corollary 2.
If $|G|$ is odd, then so is $B(G)$.

Breadths and extensions.

To find the deduced groups we have to look at extensions. The first case is the extension of an elementary abelian group by a given group.

Proposition 1. Let $B(G/N) = b_m(G/N) = n$ and $N \neq 1$ be elementary abelian of order p^k. If $B(G) = B(G/N)$ then $k = 1$ and $b_m(G/N) = b_{pm}(G)$

Proof. By definition, $mn = L_m(G/N)$. Since N is elementary abelian of order p^k, we have $L_m(G) \leq mnp^k \leq L_{mp}(G)$ and $B(G) \geq b_{mp}(G) \geq mp^{k-1}$. Equality is only possible for $k = 1$ and $L_{mp}(G) = pL_m(G/N)$.

Theorem 1 . If $B(G) = B(G/N)$, then N is cyclic.
Proof. Consider a Sylow 2-subgroup S of N. If $S = 1$, N is soluble. If $N \neq 1$, consider the normalizer $K = N_G(S)$. By the Frattini Lemma we have $KN = G$ and $G/N \cong K/(K \cap N)$. Now $B(G) \geq B(K) \geq B(K/(K \cap N)) = B(G/N)$ and $B(G) = B(K)$. Now $K \cap N$ is soluble and all elementary abelian quotients must be cyclic by Theorem 1. In particular, S is cyclic. This means that N is soluble, and all Sylow p - subgroups of N are cyclic. By a theorem of Zassenhaus, N/N' and N' are cyclic, also $(|N/N'|, |N'|) = 1$.
Assume $N' \neq 1$ and choose a complement D of N' in N. Then $A = N_G(D)$ is a complement of N' in G. If $x \in N'$ is nontrivial, $x^{-1}Dx \neq D$ and $x^{-1}Ax \neq A$. Let $m = |D|$ and $B(G/N) = b_n(G/N)$. Then $B(G/N) = B(G/N') = B(A) = b_{nm}(G/N')$ and there are more elements of order dividing m in G than there are in A. Consequently $b_{mn}(G) > b_{mn}(A) = B(A) = B(G/N)$ a contradiction. So $N' = 1$ and N is cyclic.

First examples.

We show the results of Meng and Shi in the light of the previous sections: The refined groups G with $B(G) = 2$ are $C_2 \times C_2$ and D_6.
The groups deduced from $C_2 \times C_2$ are $Q_8 \times C_w$, $C_2 \times C_{w2^m}$ and $\langle x, y | x^2 = y^{w2^{m+2}} = [x, y]^2 = 1\rangle$; here w is odd, $w \geq 1$.
The groups deduced from D_6 are $\langle x, y | x^3 = y^{2t} = xy^{-1}xy = 1\rangle$ where $t \geq 1$ is prime to 3.
The refined groups with $B(G) = 3$ are $C_3 \times C_3,\ D_6 \times C_3,\ D_8,\ D_{10}$ and $Alt(4)$.

The groups deduced from $C_3 \times C_3$ are
$\langle x, y | x^3 = y^{9k} = [x, y]^3 = 1 \rangle$ and $C_3 \times C_{3k}$ with $k \geq 1$,
the groups deduced from $D_6 \times C_3$ can be described as direct products of groups $\langle x, y | x^3 = y^{2^m} = xy^{-1}xy = 1 \rangle$ by groups C_{3w}, here $m \geq 1$ and w is odd,
the groups deduced from D_8 are $\langle x, y | x^{2k} = y^4 = yx^{-1}xy = 1 \rangle$ with k odd,
the groups deduced from D_{10} are $\langle x, y | x^2 k = y^5 = yx^{-1}xy = 1 \rangle$ with k prime to 5.
the groups deduced from $Alt(4)$ are extensions of Q_8 or $C_2 \times C_2$ by C_{3t} where t is odd, such that $SL(2, 3)$ or $Alt(4)$ are epimorphic images.

B(G) = 8.

Probably the number of refined groups G satisfying $B(G) = n$ will (as a general tendency) increase with n, apart from some influence by number theory (two non-cyclic direct factors are not possible for any prime n). We have looked at the class of groups G satisfying $B(G) = 8$, this is the smallest number where a non - soluble group occurs. We have not finished the case of refined 2-groups with $B(G) = 8$. Meng has shown that a 2 - group H with $B(H) = 4$ and $exp(H) = n$ satisfies $b_n(H) = 4$. (The converse is not true: $b_8(Hol(C_8)) = 4$ but $b_2(Hol(C_8)) = 8$.)

Refined groups G with $B(G) = 8$ are nilpotent if and only if they are 2-groups. Here is the list of the others.

(A) $(7||G|:)$

$D_{28}, LF(8) \times C_2,$

(B) $(5||G|:)$

$Alt(5), D_{30}, Hol(C_5) \times C_2,$

(C) $(9||G|:)$

$LF(9), D_6 \times D_6,$

(D) $(|G| = 2^n 3:)$

$Alt(4) \times C_2 \times C_2, SL(2,3) \times C_4,$

$\langle(1,2,3),(3,4)(5,6,7,8)\rangle \subseteq Alt(8),$

split extensions of C_3 by refined groups H with $B(H) = 4$.

Questions, Problems.

(I)If $B(G/N) = (G)$, is $N \subseteq Z(G)$? - Answer: no.

Counterexample :

$U = \langle a, b, c, d\rangle$ with the relations

$$a^2 = c^{17} = d^{17} = b^{15} = [c, d] = (ab)^2 = 1,$$
$$a^{-1}bab = a^{-1}cad^{-1} = a^{-1}dacd = 1,$$

possesses a normal subgroup $V = \langle b^3\rangle$. Now

$$b_3(U) = b_3(U/V) = 193; b_{17}(U) = b_{17}(U/V) = 17; b_2(U) = 128;$$

$$b_2(U/V) = 26; b_{51}(U) = b_{51}(U/V) = 17; b_6(U) = 139; b_6(U/V) = 105.$$

So $B(U) = B(U/V)$ and $Z(U) = 1$

(II) For a finite group G, will there be a number n such that $B(G) = b_n(G)$ with $\langle\{x \in G|x^n = 1\}\rangle = G$? - Answer: no. See above.

(III) To estimate the amount of the required work, an answer to the following would be interesting: How many pairwise non-isomorphic refined groups of breadth n are there ? A weaker version: If $B(G) = n$ and G is refined, find $p(n)$ (a polynomial for instance) such that $|G| < p(n)$?
Notice: for simple groups $PSL(2, q)$ and $Alt(m)$ we have $B(G)^2 > |G|$. Guralnik and Malle have shown for finite simple groups G that there are conjugacy classes C, D such that the product CD is equal to G or $G \setminus \{1\}$. This means $L_m(G)^2 > |G|$ for suitable m, not necessarily $b_m(G)^2 > |G|$.
For primes p we have for $G = Hol(C_p) \times C_p$ the inequality $B(G)^3 = p^3 > |G|$. Is that the general bound ?

Thank you for your attention.