Ruling out (160,54,18) difference sets in some nonabelian groups (with Jason Alexander, Rajalakshmi Balasubramanian, Kimberly Monahan, Harriet Pollatsek, and Ashna Rubina Sen) J. Combin. Designs 8 (2000), no. 4, 221--231. Publisher's official version: http://dx.doi.org/10.1002/1520-6610(2000)8:4<221::AID-JCD1>3.0.CO;2-6, Open Access version: http://kuscholarworks.ku.edu/dspace/.

Ruling out $(160, 54, 18)$ difference sets in some nonabelian groups

Alexander, Balasubramanian, Martin, Monahan, Pollatsek and Sen*

August 17, 2003

Abstract

We prove the following theorems.

Theorem A. *Let G be a group of order 160 satisfying one of the following conditions. (1) G has an image isomorphic to $D_{20} \times Z_2$ (for example, if $G \simeq D_{20} \times K$). (2) G has a normal 5–Sylow subgroup and an elementary abelian 2–Sylow subgroup. (3) G has an abelian image of exponent 2, 4, 5 or 10 and order greater than 20. Then G cannot contain a $(160, 54, 18)$ difference set.*

Theorem B. *Suppose G is a nonabelian group with 2–Sylow subgroup S and 5–Sylow subgroup T and contains a (160, 54, 18) difference set. Then we have one of three possibilities. (1) T is normal, $|\phi(S)| = 8$, and one of the following is true: (a) $G = S \times T$ and S is nonabelian; (b) G has a D_{10} image; or (c) G has a Frobenius image of order 20. (2) G has a Frobenius image of order 80. (3) G is of index 6 in $A\Gamma L(1, 16)$.*

To prove the first case of Theorem A, we find the possible distribution of a putative difference set with the stipulated parameters among the cosets of a normal subgroup using irreducible representations of the quotient; we show that no such distribution is possible. The other two cases are due to others. In the second (due to Pott) irreducible representations

*Support is gratefully acknowledged from the National Science Foundation Research Experiences for Undergraduates program, the Pew Charitable Trusts via the New England Consortium for Undergraduate Science Education, and the Howard Hughes Medical Foundation. Most of this work was done under Harriet Pollatsek's supervision in the summer 1994 undergraduate mathematics research institute at Mount Holyoke College. The other authors are the (then) undergraduate researchers: Jason Alexander '95, Lewis and Clark College, in the doctoral program in the philosophy and foundations of mathematics at UC Irvine; Rajalakshmi Balasubramanian '96, Mount Holyoke College, in the doctoral program in statistics at Harvard University; Jeremy Martin '96, Harvard University, in the doctoral program in mathematics at UC San Diego; Kimberley Monahan '95, College of the Holy Cross, now teaching high school mathematics; Ashna Sen '96, Mount Holyoke College, who completed a master's degree in geophysics at Stanford University.

of the elementary abelian quotient of order 32 give a contradiction. In the third (due to an anonymous referee), the contradiction derives from a theorem of Lander together with Dillon's "dihedral trick." Theorem B summarizes the open nonabelian cases based on this work.

1 Introduction.

Attention was drawn to the difference set parameters $(160, 54, 18)$ by Pott [11] and Smith [14] in 1993 because of the (then) recent discovery of a new symmetric design with those parameters [16]. Consequently, in the summer of 1994 the authors considered the possibility of a $(160, 54, 18)$ difference set in the group $D_{20} \times Z_2^3$. Using representations of D_{20}, we were able to show that no such difference set can exist. Actually, the 1994 work shows something stronger: If G has an image isomorphic to $D_{20} \times Z_2$, then no $(160, 54, 18)$ difference set exists in G. Since every group of order 8 contains a normal subgroup of order 4, this rules out a $(160, 54, 18)$ difference set in $D_{20} \times K$ for *every* choice of K of order 8.

Subsequently, Pollatsek was shown two much shorter proofs. An anonymous referee pointed out that a theorem of Lander excludes a $(160, 54, 18)$ difference set in any group having an abelian image G/N of order greater than 20 and exponent 2, 4, 5 or 10; by Dillon's "dihedral trick" [2], this gives nonexistence for any group with a $D_{20} \times Z_2$ image. In a personal communication [12], Pott gave a third proof of nonexistence for the original 1994 theorem, using representations of Z_2^5 to rule out a $(160, 54, 18)$ difference set in any group with a Z_2^5 image. In this note, we sketch all three proofs as a way of illustrating the diversity of methods that can be brought to bear on such questions. We summarize their consequences by stating the following result.

Theorem A. *Let G be a group of order 160 satisfying one of the following conditions.*

1. *G has an image isomorphic to $D_{20} \times Z_2$ (for example, if $G \simeq D_{20} \times K$).*
2. *G has a normal 5–Sylow subgroup and an elementary abelian 2–Sylow subgroup.*
3. *G has an abelian image of exponent 2, 4, 5 or 10 and order greater than 20.*

Then G cannot contain a $(160, 54, 18)$ difference set.

Using the program GAP [13], we determine that there are 51 groups of order 32 and 238 groups of order 160, of which 7 are abelian. Nonexistence in the abelian cases was shown by work of Kopilovich [7] and Ma and Schmidt [10]. The open nonabelian cases are summarized by Theorem B. We write $\phi(S)$ for the Frattini subgroup of S.

Theorem B. *Suppose G is a nonabelian group with 2–Sylow subgroup S and 5–Sylow subgroup T and contains a (160, 54, 18) difference set. Then we have one of three possibilities.*

1. *T is normal, $|\phi(S)| = 8$, and one of the following is true.*
   (a) *$G = S \times T$ and S is nonabelian;*
   (b) *G has a D_{10} image; or*
   (c) *G has a Frobenius image of order 20.*
2. *G has a Frobenius image of order 80.*
3. *G is of index 6 in $A\Gamma L(1, 16)$.*

Recently, Smith and Ong [15] have ruled out case (2) of Theorem B, and Liebler [9] has ruled out case (1c).

2 Preliminaries

Notation. Throughout, we use Z_m to denote the cyclic group of order m, D_{2m} to denote the dihedral group of order $2m$, and Z to denote the ring of integers, Q the rational numbers, and C the complex numbers. We always write the group operation multiplicatively to distinguish it from the addition in the integral group ring ZG. The ring of $n \times n$ matrices with entries in a field F is denoted $M(n, F)$. We use the same symbol S to represent a subset of G and also to represent the sum $S = \sum_{s \in S} s$ in ZG, and we write $S^{(m)} = \sum_{s \in S} s^m$.

2.1 Results on Difference Sets

In this section we collect the facts about difference sets that we will use. All are well-known and many are easily proved. Useful references are [6] and [8]. A (v, k, λ) *difference set* is a subset D of cardinality k in a finite group G of order v such that every non-identity element of G can be expressed exactly λ times as the "difference" df^{-1} where d and f are distinct elements of D. The *order* of the difference set is $n = k - \lambda$.

Proposition 1.1 *Let G be a group and D a (v, k, λ) difference set in G. Then $(v - 1)\lambda = k(k - 1)$.*

Proposition 1.2 [8, Prop. 4.3] *A subset D of a group G is a (v, k, λ) difference set if and only if the equation $DD^{(-1)} = n \cdot 1 + \lambda G$ holds in the integral group ring ZG, where 1 is the identity element of G.*

Let ϕ be a representation of G of degree m, and also write ϕ for the natural extension of ϕ to a ring homomorphism from ZG to $M(m, C)$,. Applying this ring homomorphism to the equation in Proposition 1.2, we obtain the following result (see [1]).

Proposition 1.3 *Assume D is a (v, k, λ) difference set in a group G.*

Ruling out (160,54,18) difference sets in some nonabelian groups (with Jason Alexander, Rajalakshmi Balasubramanian, Kimberly Monahan, Harriet Pollatsek, and Ashna Rubina Sen) J. Combin. Designs 8 (2000), no. 4, 221--231. Publisher's official version: http://dx.doi.org/10.1002/1520-6610(2000)8:4<221::AID-JCD1>3.0.CO;2-6, Open Access version: http://kuscholarworks.ku.edu/dspace/.

1. *If ϕ is a non-trivial linear representation of G and $z = \phi(D)$, then $z \in Z[\zeta]$ for some primitive root of unity ζ, and $z\overline{z} = n$.*

2. *Let ϕ be an irreducible (without loss of generality, unitary) representation of G of degree ≥ 2, and let $M = \phi(D)$. Then $M\overline{M}^T = nI$, and the entries of M are in $Z[\zeta]$ for some primitive root of unity ζ.*

Proposition 1.4 *Suppose D is a difference set in a group G with normal subgroup N, let ϕ be a representation of G/N, and also denote by ϕ the representation of G defined by $\phi(g) = \phi(gN)$. Let $\{g_iN\}$ be the distinct cosets of G/N, and let $v_i = |D \cap g_iN|$. Then $\phi(D) = \sum_i v_i\phi(g_i)$.*

The $\{v_i\}$ are called the *intersection numbers* modulo N, and they satisfy the following useful relation (even if N is not normal).

Proposition 1.5 *Let D be a (v, k, λ) difference set in a group G, and let N be a subgroup of G. If $|N| = s$ and $v_i = |D \cap g_iN|$, where the g_iN vary over the distinct cosets of G/N, then $\sum\limits_i v_i^2 = n + \lambda s$.*

Much of our analysis involves assuming that a (v, k, λ) difference set D exists and determining the intersection numbers v_i for various choices of the normal subgroup N. Since the v_i are non-negative integers whose sum is k, there are only finitely many possible choices for the v_i.

2.2 Results from number theory

Proposition 2.1 *Let ζ be a primitive p^{th} root of unity, with p prime. Suppose $\sum a_i\zeta^i = 0$, for $a_i \in Q$. Then $a_0 = a_1 = \cdots = a_{p-1}$.*

Theorem 2.2 [4, Thm. 2, p. 180] *In the ring of integers in an algebraic number field, every ideal can be written uniquely as a product of prime ideals. In particular this is true of $Z[\zeta]$, ζ a primitive root of unity.*

Theorem 2.3 [4, Thm. 2, p. 196] *Let ζ be a primitive m^{th} root of unity, and let $R = Z[\zeta]$. Let p be a prime, and assume $p \not| m$. Let f be the order of p modulo m; that is, f is the least positive integer so that $p^f \equiv 1 \mod m$. Let pR be the ideal generated by p in R . Then in R, $pR = P_1P_2 \ldots P_g$, where the P_i are distinct prime ideals, with $g = \phi(m)/f$ (where ϕ denotes the Euler phi function).*

Proposition 2.4 [5, Ex. 28.9, p.472] *Let ζ be a primitive m^{th} root of unity, and let $R = Z[\zeta]$. If $u \in R$ and $u\overline{u} = 1$, then $u = \pm\zeta^\ell$ for some integer ℓ.*

Proposition 2.5 *Let ζ be a primitive 5^{th} root of unity, and let $R = Z[\zeta]$. Let $z \in R$ with $z\overline{z} = 36$. Then $z = \pm 6\zeta^\ell$ for some integer ℓ.*

Proof: By 2.3, $2R$ and $3R$ are prime ideals; moreover, they are fixed by complex conjugation. Let $z \in R$, and assume $z\overline{z} = 36$. Then we have $zR\overline{z}R = z\overline{z}R = 36R = (2R)^2(3R)^2$. ¿From this it follows that $zR = \overline{z}R = (2R)(3R) = 6R$. But this means that $z = 6u$ for some $u \in R$ with $u\overline{u} = 1$, so 2.4 tells us that $z = \pm 6\zeta^\ell$ for some integer ℓ, as claimed. □

Ruling out (160,54,18) difference sets in some nonabelian groups (with Jason Alexander, Rajalakshmi Balasubramanian, Kimberly Monahan, Harriet Pollatsek, and Ashna Rubina Sen) J. Combin. Designs 8 (2000), no. 4, 221--231. Publisher's official version: http://dx.doi.org/10.1002/1520-6610(2000)8:4<221::AID-JCD1>3.0.CO;2-6, Open Access version: http://kuscholarworks.ku.edu/dspace/.

3 The proof using representations of D_{20}

Theorem 3.1 *If $G/N' \simeq D_{20} \times Z_2$ for some normal subgroup N', then G cannot contain a $(160, 54, 18)$ difference set.*

Proof: Note first that $G/N' \simeq D_{20} \times Z_2$ implies that G has an image isomorphic to D_{20}, say $G/N \simeq D_{20}$ and also an image G/N_1 of order 2. Assume that G does in fact contain a non-trivial $(160, 54, 18)$ difference set D. Then it is easily seen that without loss of generality we may assume $|D \cap N_1| = 24$ and $|D \cap gN_1| = 30$ are the two intersection numbers for D modulo N_1.

Set up notation so that $D_{20} = \langle x, y : x^{10} = y^2 = 1,\ x^y = x^{-1} \rangle$. Let $v_{ij} = |D \cap x^i y^j|$ be the corresponding 20 intersection numbers for D mod N, and let ζ be a primitive 5^{th} root of unity. The irreducible 2-dimensional representations of G/N have the form

$$\phi(x) = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} \quad \phi(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

where $\alpha = (-\zeta)^m$ for some positive integer m. Then

$$M = \phi(D) = \begin{bmatrix} \sum v_{i0}\alpha^i & \sum v_{i1}\alpha^i \\ \sum v_{i1}\alpha^{-i} & \sum v_{i0}\alpha^{-i} \end{bmatrix} = \begin{bmatrix} A & B \\ \overline{B} & \overline{A} \end{bmatrix}$$

By 1.3, $M \times \overline{M}^T = 36I$. From this we get $A\overline{A} + B\overline{B} = 36.$, and either $A\overline{A} = 36$ and $B\overline{B}$ =0, or vice versa. In the first instance, all the v_{i1} are equal and all but one of the v_{i0} are equal, with the tenth one differing by ± 6, and vice versa in the second instance.

Specifically, we examine the cases where $\alpha = \zeta^2$ and $\alpha = -\zeta$. In the first case we label the first row of M by $[Q, R]$, and in the second by $[S, T]$. We then have the equations

$$\begin{aligned}
Q &= (v_{00} + v_{50}) + (v_{10} + v_{60})\zeta^2 + (v_{20} + v_{70})\zeta^4 + (v_{30} + v_{80})\zeta + (v_{40} + v_{90})\zeta^3 \\
R &= (v_{01} + v_{51}) + (v_{11} + v_{61})\zeta^2 + (v_{21} + v_{71})\zeta^4 + (v_{31} + v_{81})\zeta + (v_{41} + v_{91})\zeta^3 \\
S &= (v_{00} - v_{50}) + (v_{60} - v_{10})\zeta^2 + (v_{20} - v_{70})\zeta^4 + (v_{80} - v_{30})\zeta + (v_{40} - v_{90})\zeta^3 \\
T &= (v_{01} - v_{51}) + (v_{61} - v_{11})\zeta^2 + (v_{21} - v_{71})\zeta^4 + (v_{81} - v_{31})\zeta + (v_{41} - v_{91})\zeta^3
\end{aligned}$$

We may assume $\sum v_{i0} = 24$ and $\sum v_{i1} = 30$.

Now, from a careful examination of cases, up to equivalence (by translation of D or automorphism of G), we can show that there are just two possibilities for the ordered list of intersection numbers, namely
$(v_{00}, v_{10}, \ldots, v_{10\,0}; v_{01}, v_{11}, \ldots, v_{10\,1}) =$
(1) (0, 6, 3, 3, 3, 0, 0, 3, 3, 3; 3, 3, 3, 3, 3, 3, 3, 3, 3, 3) or
(2) (0, 3, 3, 3, 3, 0, 3, 3, 3, 3; 6, 3, 3, 3, 3, 0, 3, 3, 3, 3).

Some possibilities are ruled out by 1.5; others are ruled out by considering overgroups of N and unions of cosets mod N. (For details of the argument, see the web page `www.mtholyoke.edu/~hpollats`. Note that the argument never uses any information about the structure of N.)

Finally, $G/N' \simeq D_{20} \times Z_2$, gives intersection numbers w_{ijk} with $0 \leq i \leq 10, 0 \leq j, k \leq 1$ for D. The irreducible representations of this quotient are tensor products of representations of D_{20} with those of Z_2, and, using an argument similar to the one for the v_{ij}, it can be shown that no assignment of the w_{ijk} consistent with the v_{ij} is possible, and therefore the difference set cannot exist. This establishes the first case of Theorem A. □

4 The proof using the "dihedral trick"

Theorem 4.1 *Suppose G has a normal subgroup N' of order 4 with $G/N' \simeq D_{20} \times Z_2$. Then G contains no $(160, 54, 18)$ difference set.*

The proof we present relies on results of Lander and Dillon. Before stating them, we need some definitions. Suppose a group G with a normal subgroup N has a (v, k, λ) difference set D. Write $H = G/N$, and for $h \in H$, let s_h be the size of the intersection of D with the coset h. Then $S = \sum_{h \in H} s_h h$ satisfies the ZH equation

$$SS^{(-1)} = n + \lambda |N| H$$

from which it follows that $\sum_{h \in H} s_h = k$, $\sum_{h \in H} s_h^2 = n + \lambda |N|$ (as in 1.5) and for $a \neq b \in H$, $\sum_{h \in H} s_{ah} s_{bh} = \lambda |N|$ (see [6, p. 260]). Such an element of ZH is called a (w, k, s, λ) *difference list in H*, where $|H| = w$ and $|N| = s$.

Theorem 4.2 [2, p. 16] *Let A be an abelian group, and let $H = \langle A, Q \rangle$, where $QaQ = a^{-1}$ for all $a \in A$, $Q^2 = 1$. Let $K = \langle A, \theta \rangle$, where $[\theta, a] = 1$ for all $a \in A$ and $\theta^2 \in A$. If H contains a (w, k, s, λ) difference list, then so does K. Specifically, if $S = \sum_{a \in A} u_a a + v_a Q a$ is a difference list in ZH, then $T = \sum_{a \in A} u_a a + v_a \theta a$ is a difference list in ZK with the same parameters.*

We need two further definitions. Let H be a group of order w, $H = \{h_1 = 1, h_2, \ldots, h_w\}$, and let M be a $w \times w$ matrix whose rows and columns are indexed by elements of H. If the first row of M is $(m_{h_1}, \ldots, m_{h_w})$, and the row corresponding to $x^{-1} \in H$ is $(m_{xh_1}, \ldots, m_{xh_w})$, then we say M is an *H–matrix.* We say an integer m is *semi-primitive* modulo e if $m^j \equiv -1 \pmod{e}$ for some j.

Theorem 4.3 [8, Theorem 4.17] *Let H be an abelian group of exponent e and order w, and assume that M is an integral H–matrix satisfying*

$$MM^T = xI + yJ \text{ and } MJ = JM = zJ$$

for integers x,y and z, where I is the identity matrix and J is the all–one matrix. If there exists an integer m with $m^2 | x$ and m semi-primitive modulo e, then $M \equiv aJ \pmod{m}$, where $wa \equiv z \pmod{m}$.

If $S = \sum_{h \in H} s_h h$ is a (w, k, s, λ) difference list in $H = \{h_1, \ldots, h_w\}$, then define an integral H–matrix M with first row $(s_{h_1}, \ldots, s_{h_w})$. Then the relations satisfied by the intersection numbers s_h imply

$$MM^T = nI + \lambda sJ \text{ and } MJ = JM = kJ$$

Combining this with Theorem 4.3 we get

Corollary 4.4 *Let H be an abelian group of order $w > 1$ and exponent e, and assume $S = \sum_{h \in H} s_h h$ is a (w, k, s, λ) difference list. If there is an integer m semi-primitive modulo e and with $m^2 | n$, then $s_h \equiv a \pmod{m}$ for all $h \in H$, where $wa \equiv k \pmod{m}$. Moreover, if $m|k$ and m is relatively prime to w, then $s \geq (km - n)/\lambda$.*

Proof: Only the last statement needs proof. First note that $(w, m) = 1$ and $k \equiv 0 \pmod{m}$ imply $s_h \equiv a \equiv 0 \pmod{m}$. Write $s_h = mt_h$, so $\sum_{h \in H} s_h = m \sum t_h = k$ implies $\sum t_h = k/m$. Also, $\sum s_h^2 = m^2 \sum t_h^2 = n + \lambda s$ gives $\sum t_h^2 = (n + \lambda s)/m^2$. But then $k/m = \sum t_h \leq \sum t_h^2$ gives the desired inequality. □

Note that since Corollary 4.4 applies to abelian quotients $H = G/N$, it is stronger than Lander's consequence of Theorem 4.3 [8, Theorem 4.18], which requires that G be abelian. (Also note the typographical error in [8, Theorem 4.18]: the correct conclusion is $m \leq |N|$.)

Now we can prove Theorem 4.1. Assume $G/N' \simeq H = D_{20} \times Z_2$ and G has a $(160, 54, 18)$ difference set D. By Theorem 4.2, we may assume that the abelian group $K = Z_{10} \times Z_2 \times Z_2$ has a $(40, 54, 4, 18)$ difference list with coefficients s_h equal to the H intersection numbers of the difference set D in G. If we choose $m = 3$, then we see that $m^2 = 9 | n = 18$ and $3^2 \equiv -1$ (mod $e = 10$), so by Corollary 4.4, we have $s = 4 \geq (km - n)/\lambda = (162 - 36)/18 = 7$, which is a contradiction. This gives a second proof of part (1) of Theorem A. □

This same argument gives the following theorem and extablishes part (3) of Theorem A.

Theorem 4.5 *Suppose G is a group with a $(160, 54, 18)$ difference set. If G has an abelian quotient H of exponent 2, 4, 5 or 10, then $|H| \leq 20$.*

Proof The integer $m = 3$ satisfies the hypotheses of Corollary 4.4 for $e = 2$, 4, 5 or 10, so the index of H is at most 7. □ (Note, however, that since $3^4 \equiv 1$ (mod 20), 3 is not semi-primitive modulo any multiple of 20.)

5 The proof using representations of Z_2^5

Theorem 5.1 [12] *Let G be a group of order 160 with a normal 5–Sylow subgroup N and an elementary abelian 2–Sylow subgroup. Then G does not contain a $(160, 54, 18)$ difference set.*

Proof: Suppose that G does contain a $(160, 54, 18)$ difference set D. Representations of Z_2^5 are all integer-valued (values ± 1 actually). Suppose $\{v_i\}$ are the 32 intersection numbers for D with respect to the cosets of N, so $0 \leq v_i \leq 5$ for each i, $\sum v_i = k = 54$ and $\sum v_i^2 = n + \lambda s = 36 + 18 \cdot 5 = 126$.

Form a column vector v whose coordinates are the integers v_i. Write $[\chi]$ for the 32×32 matrix of 0's and 1's which is the character table of Z_2^5. Then, because $\sqrt{n} = 6$ in our case, we may write $[\chi]v = 6z$, where the entries of the vector z are integers. By the orthogonality relations for characters, $[\chi] \times \overline{[\chi]}^T = 32I$, so we can write $v = (6/32)[\chi]^T z = (6/32)z'$, where the entries of the vector z' are also integers. Thus we have $32v_i = 6z_i'$ for each i, and therefore each v_i is divisible by 3. Since $0 \leq v_i \leq 5$, we can only have $v_i = 0$ or $v_i = 3$. Because $\sum v_i = 54$, 18 of the v_i equal 3 and 14 equal 0. But then $\sum v_i^2 = 18 \cdot 9 = 162 \neq 126$, so we have a contradiction, and G cannot contain a $(160, 54, 18)$ difference set. This establishes part (2) of Theorem A. □

Note that if $G = D_{20} \times Z_2^3$, then the rotation subgroup of D_{20} is $N \times Z_2$, where N is the unique 5–Sylow subgroup of G, and the quotient G/N is elementary abelian, so Theorem 5.1 rules out a difference set in this case.

6 The remaining nonabelian cases

Putting together the results in the preceding sections, we have the following theorem.

Theorem B. *Suppose G is a nonabelian group with 2–Sylow subgroup S and 5–Sylow subgroup T and contains a (160, 54, 18) difference set. Then we have one of three possibilities.*

1. *T is normal, $|\phi(S)| = 8$, and one of the following is true.*
   - *(a) $G = S \times T$ and S is nonabelian;*
   - *(b) G has a D_{10} image; or*
   - *(c) G has a Frobenius image of order 20.*
2. *G has a Frobenius image of order 80.*
3. *G is of index 6 in $A\Gamma L(1, 16)$.*

Proof: Write $\phi(S)$ for the Frattini subgroup of S. Note that $|\phi(S)| = 16$ implies that S is cyclic [3, Thm. 5.1.1].

We require the following lemma due to Liebler; a sketch of the proof of 6.1 follows that of Theorem B.

Lemma 6.1. [9] *Suppose G contains a $(160, 54, 18)$ difference set. Then G cannot have a cyclic image of order 32.*

First, assume that T is normal, so Lemma 6.1 rules out $|\phi(S)| = 16$. Let $\eta : S \to \mathrm{Aut}(T) \simeq Z_4$, and let $K = \ker \eta$. The possibilities are that $|K| = 32$, 16, or 8. If $|K| = 32$, elements of S commute with elements of T and S is normal also (as is $\phi(S)$). Since G is nonabelian, S is nonabelian. If $|\phi(S)| \leq 4$, then $G/\phi(S)$ is abelian of exponent 10, so G has no difference set by part (3) of Theorem A, and we have case (1a) of Theorem B. If $|K| = 16$, then $G/K \simeq D_{10}$. If $|\phi(S)| \leq 4$, then G has no difference set by part (1) of Theorem A, and we have case (1b). If $|K| = 8$, then G/K is Frobenius of order 20, and we have case (1c).

If S is normal and T is not, then G has a normal subgroup N of order 2 (the intersection with S of the kernel of the permutation representation of G on its 16 5–Sylow subgroups) and G/N is Frobenius, giving case (2).

The remaining possibility is that neither S nor T is normal. Liebler [9] has pointed out that such a group of order 160 occurs as a subgroup of $A\Gamma L(1, 16)$ of index 6. It is generated by the subgroup of order 5 of the multiplicative group $\langle \alpha \rangle$ of GF(16), the automorphism of GF(16) taking α to α^4 (together giving a dihedral group of order 10) and the elementary abelian additive group of GF(16). It can be shown, as we verify using GAP [13], that there is exactly one isomorphism type among the groups of order 160 having no normal Sylow subgroups. (A proof of this fact follows that of Liebler's lemma.) This gives case (3) and completes the proof of Theorem B. □

Remarks: Recently, Smith and Ong [15] have ruled out case (2) of Theorem B, and Liebler [9] has ruled out case (1c). Note that $|\phi(S)| = 8$ implies S has two generators [3, 5.1.1]. If one generator has order 16, then there are 7 possibilities for S, two abelian and 4 nonabelian (dihedral, semidihedral, generalized quaternion, or modular). (See [3, 5.4.4]). Using GAP [13], there are 19 isomorphism types for S if $|\phi(S)| = 8$, two of which are abelian. Case $1(a)$ includes the possibility that G has a Z_{40} image, and Smith [15] has pointed out that the automorphism group of the first (160, 54, 18) design discovered is compatible with the existence of difference set in a group with a Z_{40} image.

Sketch of proof of Lemma 6.1: Liebler's proof is based on a calculation using Maple. The logic of the calculation is straightforward. Assume that G contains a $(160, 54, 18)$ difference set and has a cyclic image of order 32 (and therefore cyclic images of order 2, 4, 8 and 16 as well). We determine the possible intersection numbers for each of these.

Arguing as in the proof of Theorem 3.1, it is easy to check that the Z_2 intersection numbers are $\{30, 24\}$ and the Z_4 intersection numbers are either $\{18, 12, 12, 12\}$ or $\{15, 15, 15, 9\}$.

The number theory for the calculation of the possible Z_8 intersection numbers is more complicated. If ζ is a primitive 8th root of unity, then the ideal in $Z[\zeta]$ generated by 3 is the product of two prime ideals, generated by $\zeta^2 + \zeta - 1$ and $\zeta^2 - \zeta - 1$ respectively; the ideal generated by 2 is the fourth power of the ideal generated by $\zeta + 1$. These factorizations are found by factoring the cyclotomic polynomial $\Phi_8(x) = x^4 + 1$ mod 3, obtaining $(x^2 + 2x + 2)(x^2 + x + 2)$, and mod 2, obtaining $(x + 1)^4$. If v_j, $j = 0, \ldots, 7$ are the intersection numbers for the Z_8 image, and if χ is the character taking the generator of Z_8 to ζ, then $d = \chi(D) = \sum_j v_j \zeta^j$ has one of three possible forms: $d = 6\zeta^\ell$, $d = 2(\zeta^2 + \zeta - 1)^2 \zeta^l$, or $d = 2(\zeta^2 - \zeta - 1)\zeta^\ell$ for some $\ell = 0, \ldots, 7$.

Each of the three cases gives an expression of the form $\sum_{j=0}^{3} c_j \zeta^j = 0$ for integers c_j, implying that the polynomial $\sum_{j=0}^{3} c_j x^j$ divides the minimum polynomial $x^4 + 1$ of ζ, which can only happen if the c_j are all zero. From this we determine that for each of the three possible forms of d, only the even Z_4 intersection numbers are compatible with the existence of a Z_8 image.

A Maple calculation produces 12 inequivalent sets of Z_8 intersection numbers. (They are listed in an appendix.) A similar argument for the Z_{16} image shows that the Z_8 intersection numbers must also be even; three sets survive: $[12, 6, 6, 6, 6, 6, 6, 6]$, $[10, 8, 6, 8, 8, 4, 6, 4]$, and $[10, 4, 6, 4, 8, 8, 6, 8]$.

Now, factoring $\Phi_{16}(x)$ mod 3 and mod 2 gives us the factorizations of the ideals generated by 2 and by 3 in $Z[\eta]$ for η a primitive 16th root of unity, and this, in turn, gives us the possible images of D under the character taking the generator of Z_{16} to η. From this, another Maple calculation gives the possible sets of Z_{16} intersection numbers. (Again, they are listed in the appendix.) As before, the existence of the Z_{32} image forces the Z_{16} intersection numbers to be even, but for *none* of the possible sets is this true. Therefore a group containing a $(160, 54, 18)$ difference set cannot have a Z_{32} image. □

Lemma 6.2. *If a group of order 160 has no normal Sylow subgroups, then it is isomorphic to a subgroup of $A\Gamma L(1, 16)$.*

Proof: First we claim that a chief series for G must have factors of size $2, 5, 16$. Since the 5–Sylow subgroups are not normal, the top and bottom factors are powers of 2. The top factor can't exceed 2, since a normal subgroup of order $2^a \cdot 5$ with $a < 4$ has a normal 5–Sylow, forcing a normal 5–Sylow in G. The bottom factor comes from a normal elementary abelian subgroup N of order 2^b for some b. A 5–Sylow subgroup T of G normalizes N, and if $b < 4$ it must centralize N; so, since $|N_G(T)| = 10$, the bottom factor must be 2 or 16. If the bottom factor were 2, we'd again find T centralizing too many elements of even order. So G has a chief series $1 \lhd N \lhd F \lhd G$, with N elementary abelian of order 16 and F of index 2.

Now we show that $G/N \simeq D_{10}$, giving the desired isomorphism. Notice that a 2–Sylow subgroup S of G cannot centralize N, for if S were (necessarily, properly) contained in the kernel of the map from G to $\mathrm{Aut}(N)$, it would follow that G and hence a 5–Sylow subgroup T of G centralizes N, contradicting $|N_G(T)| = 10$. Choose $x \in S \setminus N$ and $y \in N$ with $y^x \neq x$. If x is an involution, we have $\langle T, x\rangle = D_{10}$, and we are done. If x is not an involution, it must have order 4, implying $\langle x, y\rangle$ of order 8 contains the Klein group $\langle y, y^x\rangle$ and is therefore dihedral. But $\langle x, y\rangle \cap N = \langle y, y^x\rangle$, so there are involutions in S not in

N, and we can choose one in place of x. □

Acknowledgments: The authors thank Robert Liebler and Kenneth Smith for communicating their related work and particularly thank Robert Liebler for his help. The authors are also grateful to two anonymous referees for their thoughtful suggestions.

References

[1] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley Interscience Publ., 1962.

[2] J. Dillon, *Variations on a scheme of McFarland for Noncyclic Difference Sets*, J. of Comb. Theory A **40**, 1985, 9-21.

[3] D. Gorenstein, *Finite Groups*, Harper and Row, 1968.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, 2nd corrected printing, GTM, Springer Verlag, 1992.

[5] I.M. Isaacs, *Algebra, A Graduate Course*, Brooks Cole Publ. Co., 1994.

[6] D. Jungnickel, Difference Sets, in *Contemporary Design Theory: A Collection of Surveys*, J.H. Dinitz and D.R. Stinson eds., John Wiley and Sons, 1992.

[7] L.E. Kopilovich, *Difference sets in noncyclic abelian groups* (English translation),Kiberneticka **2**, 1989, 20-23.

[8] E.S. Lander, *Symmetric Designs: an algebraic approach*, London Math. Soc. Lecture Note Series 74, Cambridge Univ. Press, 1983.

[9] R.A.Liebler, personal communication, 1999.

[10] S.L. Ma and B. Schmidt, *Difference sets correponding to a class of symmetric designs*, Des. Codes Cryptogr. **10**, 1997, 223-236.

[11] A. Pott, *Quasiregular collineation groups of projective planes*, Difference Set Meeting, Ohio State University, 1993.

[12] A. Pott, personal communication, 1995.

[13] M. Schönert *et al*, *GAP—Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, Rheinishch-Westfälische Technische Hochschule, Aachen, Germany, version 4r1, 1999.

[14] K.W. Smith, *On Extending Lander's Table of Difference Sets: Searching for non-abelian difference sets*, preprint, 1992.

[15] K.W. Smith, personal communication, 1999.

[16] E. Spence, V.D. Tonchev, and T. van Trung, *A symmetric 2-(160,54,18) design*, J. of Comb. Designs **1**, 1993, 65-68.

Appendix. The other 9 possible Z_8 interesection numbers are, up to equivalence (via cyclic shifts and autmorphisms of Z_8), among the following 8-tuples. [9,9,6,6,9,3,6,6], [9,6,9,6,9,6,3,6], [9,6,6,9,9,6,6,3], [9,4,5,8,9,8,7,4], [7,6,4,5,11,6,8,7], [11,7,4,6,7,5,8,6], [9,8,5,4,9,4,7,8], [11,6,8,5,7,6,4,7], [7,7,8,6,11,5,4,6].

The possible Z_{16} intersection numbers are, up to equivalence, among the following 23 16-tuples.

[9,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3], [0,3,3,3,3,3,3,6,6,3,3,3,3,3,3,6],
[0,3,6,3,3,3,3,3,6,3,6,3,3,3,3,3], [0,3,3,3,6,3,3,3,6,3,3,3,6,3,3,3],
[2,3,5,3,6,3,5,3,4,3,1,3,6,3,1,3], [2,3,1,3,3,6,1,3,4,3,5,3,3,6,5,3],
[2,6,1,3,3,3,1,3,4,6,5,3,3,3,5,3], [1,3,2,3,8,3,3,3,5,3,4,3,4,3,3,3],
[7,3,1,3,3,3,1,3,5,3,5,3,3,3,5,3], [8,4,3,4,5,2,3,2,7,4,3,4,5,2,3,2],
[0,4,4,2,3,2,5,4,6,4,4,2,3,2,5,4], [3,2,5,2,5,4,5,4,5,2,1,2,5,4,1,4],
[3,4,5,4,5,2,5,2,5,4,1,4,5,2,1,2], [0,5,4,3,2,4,1,3,4,5,4,3,6,4,3,3],
[0,3,1,4,6,3,4,5,4,3,3,4,2,3,4,5], [6,2,4,2,3,4,3,4,2,2,2,2,7,4,3,4],
[6,4,3,4,7,2,4,2,2,4,3,4,3,2,2,2], [6,4,1,4,4,2,1,2,4,4,5,4,4,2,5,2],
[6,2,1,2,4,4,1,4,4,2,5,2,4,4,5,4], [0,5,3,3,6,4,2,3,4,5,5,3,2,4,2,3],
[0,3,2,4,2,3,3,5,4,3,2,4,6,3,5,5].