Polynomial-Time Testing and Pronormality in Solvable Quotients of Permutation Groups

Arnold D. Feldman

CIS-TR-93-16
June 25, 1993

Abstract

We present polynomial-time algorithms for computations involving pronormal subgroups of solvable quotient groups $G= G/K$, where G is a permutation group. In particular, we show that it is possible to determine in polynomial time whether or not all subgroups of G are pronormal, i.e, whether G is a t-group.

We also present polynomial-time algorithms for determining whether a subgroup U of G is pronormal in G, and to compute the normalizer $N_G(U)$ if U is pronormal in G.

Department of Computer and Information Science
University of Oregon

Polynomial-Time Testing and Pronormality in Solvable Quotients of Permutation Groups

Arnold D. Feldman [1]
Department of Mathematics
Franklin and Marshall College
Lancaster, PA 17604-3003

June 25, 1993

[1] Research carried out at the University of Oregon during the author's Sabbatical Leave.

Introduction

If G is a group and U is a subgroup of G, we say U is *pronormal* in G, denoted U pr G, if for each element g of G, U is conjugate to U^g via an element of $<U,U^g>$. Pronormal subgroups include Sylow subgroups, Hall subgroups, maximal subgroups, and Carter subgroups. A solvable *t-group* is a solvable group in which normality is a transitive property, i.e., a solvable group in which every subnormal subgroup is normal. These turn out to be the solvable groups in which every subgroup is pronormal [Fe].

In [KL], Kantor and Luks describe a tool kit for obtaining polynomial-time algorithms for determining various subgroups and checking various properties of finite permutation groups and their quotients. Some of their results are detailed below, in Lemma 0.1. The purpose of this note is to illustrate the power of this tool kit when combined with information about solvable t-groups and about pronormal subgroups of solvable groups.

Of particular interest here are results concerning the normalizer of a subgroup of a group that is a solvable quotient of a group of permutations. In [KL], polynomial-time algorithms for computing normalizers are described for two special cases: when the group is nilpotent, and when the subgroup is a Sylow or Hall subgroup. It is important to note that in [Lu2], Luks presents more complex and difficult methods that make it possible to compute in polynomial time the normalizer of an arbitrary subgroup of a solvable quotient of permutation groups. In this paper, we show how to exploit special properties of t-groups and of pronormal subgroups to compute certain normalizers using the methods of [KL], without having to resort to the more advanced techniques of [Lu2].

First, in Section 1, we use the techniques of [KL] but not of [Lu2] to obtain, in Theorem 1.1, a polynomial-time algorithm for checking whether a quotient of permutation groups is a solvable t-group. For the special case of nilpotent quotients of permutation groups, in addition to describing polynomial-time algorithms for computing normalizers of subgroups of such groups, Kantor and Luks present a polynomial-time algorithm for determining whether two subgroups are conjugate, and if so, obtaining an element conjugating one to the other. In Proposition 1.4, we show how to adapt these algorithms to apply to solvable t-groups that are quotients of permutation groups.

In Section 2 we concentrate on the pronormality of individual subgroups of a solvable quotient of permutation groups. We begin by obtaining, in Theorem 2.1, a criterion for pronormality of a subgroup in terms of the index of its normalizer. Then in

Theorem 2.3, again using the results of [KL] but not of [Lu2], we describe a polynomial-time procedure for simultaneously determining whether a subgroup is pronormal and for computing its normalizer.

0. Notation and Tool Kit

Let G be a group of permutations on a set Ω of size n, and K be a normal subgroup of G. Let **G** denote G/K, and similarly let **A** denote A/K for any subgroup A of G containing K. When we refer to a *polynomial-time* algorithm for **G**, we mean an algorithm whose running time is polynomial in n. Note that |**G**| could be as large as n!, much larger than n, although the prime factors of |**G**| are all less than or equal to n.

In Lemma 0.1, we present a summary of the propositions from [KL] that we will use below. The proposition numbers from P1 to P16 labelling the parts of Lemma 0.1 refer to the sources of these parts in that work.

Note In the Lemma and below, the statement "find a subgroup **X** of **G**" means "obtain generators of **X**".

Lemma 0.1 Let **G** denote G/K as above. Then there exists a polynomial-time algorithm for each of the following problems.

(i) Find |**G**|. [P1]

(ii) Given a subset S of **G**, find the normal closure of S in **G**, i.e. the smallest normal subgroup of **G** containing S. [P3(i)].

(iii) Given subgroups **A** and **B** of **G** solvable, find $\mathbf{A} \cap \mathbf{B}$. [P4(iii)]

(iv) Given a subgroup **A** of **G** solvable, find $C_{\mathbf{A}}(\mathbf{B})$. [P7(i)]

(v) Given a subgroup **B** of **G** nilpotent, find $N_{\mathbf{G}}(\mathbf{B})$. [P8(i)]

(vi) Given subgroups $\mathbf{B}_1$ and $\mathbf{B}_2$ of **G** nilpotent, determine whether or not $\mathbf{B}_1$ and $\mathbf{B}_2$ are conjugate in **G**, and if so, find g in **G** such that $\mathbf{B}_1^g = \mathbf{B}_2$. [P8(ii)]

(vii) Find a composition series for **G**. [P10(iii)]

(viii) (a) If H is normal in G, test whether H is a minimal normal subgroup, and if not, find N normal in G such that $1 < N < H$. [P11(i), (ii)]

(b) Find a chief series for G. [P11(iii)]

(ix) If G is solvable and π is a set of primes

(a) find a Hall π-subgroup of G containing a given π-subgroup H of G. [P13(i); Remark (ii), p. 13]

(b) given Hall π-subgroups H_1 and H_2 of G, find g in G such that $P_1^g = P_2$. [P13(ii); Remark (ii), p. 13]

(c) given a Hall π-subgroup H of L, where L is normal in G, find $N_G(H)$. [P13(iii); Remark (ii), p.13]

(x) Find the derived series, lower central series, and upper central series of G. [P14]

(xi) Find the *socle* of G, i.e., the subgroup generated by all minimal normal subgroups of G. [P15(i)]

(xii) Find the intersection of all maximal normal subgroups of G. [P15(ii)]

(xiii) For any collection Σ of simple groups, find $O_\Sigma(G)$ and $O^\Sigma(G)$. (Here $O_\Sigma(G)$ denotes the largest normal subgroup of G each of whose composition factors is in Σ, and $O^\Sigma(G)$denotes the smallest normal subgroup of G such that each composition factor of $G/O_\Sigma(G)$ is in Σ.) [P16]

When we refer below to a part of this Lemma, we will write only the part number. Thus (i) refers to Lemma 0.1(i), which is actually [KL, P1].

1. t-groups

Gaschutz [Ga] has described the structure of solvable t-groups. Recently the author [Fe] has shown that a solvable group is a t-group if and only if all of its subgroups are pronormal.

Our first goal is to establish the following:

<u>Theorem 1.1</u> There is a polynomial time algorithm to determine if $\mathbf{G}$ is a solvable t-group.

We begin by stating the parts we need of two results of Gaschutz, which apply to all finite groups, whether or not they are described as permutation groups. Here a group is called *Dedekind* if all of its subgroups are normal, and G^{N} denotes the smallest normal subgroup of G with G/G^{N} nilpotent.

<u>Satz 1</u> [Ga] If G is a solvable t-group, and $L=G^{N}$, then:

a) G/L is Dedekind,

b) $|L|$ is odd,

c) L is abelian,

d) $(|G/L|,|L|) = 1$, and

e) for any automorphism σ on L induced by an inner automorphism of G, there exists an integer, m, such that $x^{\sigma} = x^{m}$ for all $x \in L$.

<u>Satz 2</u> If G is a finite group with a normal subgroup L satisfying a), d), and e) described above, then G is a solvable t-group.

Now suppose that G and $\mathbf{G}$ are as described above. Then the subgroup $\mathbf{L} = \mathbf{G}^{N}$, which is the minimal element of the lower central series of $\mathbf{G}$, can be computed in polynomial time by (x). By (i), we can compute both $|\mathbf{G}|$ and $|\mathbf{G}^{N}|$ in polynomial time, so we can easily check d). Thus to check in polynomial time whether $\mathbf{G}$ is a solvable t-group, we need only devise schemes for checking a) and e) in polynomial time.

Note that we have generators for $\mathbf{L}$, which equals L/K for some normal subgroup L of G, and we have generators for K. We can combine these to obtain generators for L, so we can apply Lemma 0.1 to G/L or to L/K. But $\mathbf{G}/\mathbf{L}$ is isomorphic to G/L, so any structural property we can obtain for G/L using that Lemma is also possessed by $\mathbf{G}/\mathbf{L}$. Similarly, we can use the Lemma for $L/K = \mathbf{L}$. In fact, the former argument works for any normal subgroup of $\mathbf{G}$ whose generators we can compute in polynomial time, and the latter argument works for any subgroup of $\mathbf{G}$ we can obtain in polynomial time, whether or not it is normal in $\mathbf{G}$.

In particular, then, the following result for general G as defined above implies that we can check a) in polynomial time.

Lemma 1.2 There is a polynomial time algorithm to determine whether G is a Dedekind group.

Proof Every abelian group is Dedekind, and non-abelian Dedekind groups are called *Hamiltonian*. Because by (x) we can check whether G is abelian, we need only show that we can check in polynomial time whether G is Hamiltonian.

Now a finite group is Hamiltonian if and only if it is the direct product of an abelian group of odd order, a quaternion group, and an elementary abelian 2-group [Ha, Theorem 12.5.4]. Thus G is Hamiltonian if and only if:

i) $|G| = |O_2(G)||O^2(G)|$,

ii) $O^2(G)$ is an abelian Hall 2'-subgroup of G, and

iii) $O_2(G)$ is the direct product of a quaternion group and an elementary abelian 2-group.

We can obtain each of $O^2(G)$ and $O_2(G)$ in polynomial time by (xiii), with Σ consisting of just the cyclic group of order 2. Thus i) can be checked using (i).

We can compute $|O^2(G)|$ by (i), easily check whether it is odd, and check whether $O^2(G)$ is abelian by (x). Checking whether $|G|/|O^2(G)|$ is a power of 2 takes at most $\log|G|$ divisions by 2, where $|G| \leq n^n$, so $\log|G| \leq n^2$. Thus we can check ii) in polynomial time.

Checking iii) is more complicated. Let $T = O_2(G)$. Now we can compute the center Z(T) by (x) and the socle soc(T) by (xi). Suppose for the moment that $T = Q \times E$, where Q is a quaternion group and E is elementary abelian. Note that any nontrivial element of E generates a minimal normal subgroup of T of order 2, and Z(Q) is also a minimal normal subgroup of T of order 2. Then $\mathrm{soc}(T) \leq Z(Q) \times E$. But if N is minimal normal in T and not contained in $Z(Q) \times E$, then $Z(Q) \times E \times N$ is a proper subgroup of T because T is not abelian. Then $|T: Z(Q) \times E| = 4$ implies N is of order 2. It is easy to see that the elements of order 2 in T are all in $Z(Q) \times E$, a contradiction. Thus $\mathrm{soc}(T) = Z(Q) \times E = Z(T)$, an elementary abelian group of index 4 in T.

Furthermore, by (xii) we can compute the intersection of all maximal normal subgroups of T, which in the nilpotent group T is $\Phi(T)$, the intersection of all the maximal subgroups of T. Now $T/\Phi(T)$ is the largest elementary abelian quotient group of T, so if $T = Q \times E$, $\Phi(T) = \Phi(Q) = Z(Q)$, the unique subgroup of Q of order 2. Then $\Phi(T) = Z(Q) \leq \mathrm{soc}(T)$. Note that we can check whether the 2-group soc(T) is elementary abelian by checking whether its generators commute with each other and are of order 2, or by checking whether $\Phi(\mathrm{soc}(\mathbf{T})) = 1$. Thus the first step in checking iii) is checking whether $\mathrm{soc}(\mathbf{T}) = Z(\mathbf{T})$, $\Phi(\mathrm{soc}(\mathbf{T})) = 1$, and $\Phi(\mathbf{T}) \leq \mathrm{soc}(\mathbf{T})$.

Hence we may assume in checking iii) that $\mathrm{soc}(\mathbf{T})=Z(\mathbf{T})$ is elementary abelian, $|\Phi(\mathbf{T})| = 2$, and $\mathrm{soc}(\mathbf{T})$ is of index 4 in $\mathbf{T}$.

Let $\mathbf{A} = \mathrm{soc}(\mathbf{T})$ and $\mathbf{B} = \Phi(\mathbf{T})$, a subgroup of order 2 of the elementary abelian group $\mathbf{A}$. Let $\mathbf{A} = A/K$ and $\mathbf{B} = B/K$, so B is normal in A. As remarked above, we can apply Lemma 0.1 to A/B. In particular, by (vii), we can obtain a composition series $B/B = B_0/B < B_1/B < B_2/B < \ldots < B_w/B = A/B$ for the elementary abelian A/B, where $2^w = |A/B| = |\mathbf{A}/\mathbf{B}|$. For each B_i/B, choose one generator Bb_i that is not contained in B_{i-1}/B. (We know that the number of generators obtained for B_i/B is at most w, less than n^2.) Thus $<Bb_1> = B_1/B$ and $<Bb_1,Bb_2,\ldots,Bb_w> = A/B$. Therefore, $B<b_1,b_2,\ldots,b_w> = A$. Hence $(B/K)[<Kb_1,Kb_2,\ldots,Kb_w>] = A/K$; i.e., $\mathbf{B}<Kb_1,Kb_2,\ldots,Kb_w> = \mathbf{A}$. Let $\mathbf{W} = <Kb_1,Kb_2,\ldots,Kb_w>$, so $|\mathbf{A}| = |\mathbf{B}|\,|\mathbf{W}| / |\mathbf{B} \cap \mathbf{W}|$. But each Kb_i is of order 2 in the elementary abelian group $\mathbf{A}$, so $|\mathbf{W}| \leq 2^w = |\mathbf{A}/\mathbf{B}|$. Hence $|\mathbf{B} \cap \mathbf{W}| =1$, and $\mathbf{A} = \mathbf{B} \times \mathbf{W}$.

Note that $\mathbf{W} \leq \mathbf{A}$ and $\mathbf{B} = \Phi(\mathbf{T}) \cap \mathbf{A}$, so $|\Phi(\mathbf{T}) \cap \mathbf{W}| = 1$. We can check whether $\mathbf{W}$ is normal in $\mathbf{T}$ using (ii). If not, $\mathbf{T}$ is not Dedekind, so we assume $\mathbf{W}$ is normal in $\mathbf{T}$. Suppose again that $\mathbf{T} = \mathbf{Q} \times \mathbf{E}$ for some quaternion group $\mathbf{Q}$ and elementary abelian 2-group $\mathbf{E}$. Then $\mathbf{Q} \cap \mathbf{W} \leq \mathrm{soc}(\mathbf{Q}) = Z(\mathbf{Q}) = \mathbf{B}$, so $|\mathbf{Q} \cap \mathbf{W}| = 1$. Also, $\mathbf{B} \times \mathbf{E} = \mathbf{A} = \mathbf{B} \times \mathbf{W}$, so $|\mathbf{W}| = |\mathbf{E}|$. Thus $|\mathbf{QW}| = |\mathbf{QE}| = |\mathbf{T}|$, so $\mathbf{T} = \mathbf{Q} \times \mathbf{W}$, and $\mathbf{T}/\mathbf{W}$ is a quaternion group. Thus $\mathbf{T} = \mathbf{Q} \times \mathbf{E}$ for some quaternion group $\mathbf{Q}$ and some elementary abelian group $\mathbf{E}$ if and only if $\mathbf{T}/\mathbf{W}$ is a quaternion group and $\mathbf{W}$ is complemented in T.

It is easy to check in polynomial time whether $\mathbf{T}/\mathbf{W}$ is a quaternion group. We simply check whether or not $\mathbf{T}/\mathbf{W}$ is a group of order 8 that has precisely one element of order 2 and more than 2 elements of order 4. Then we may assume that $\mathbf{T}/\mathbf{W}$ is a quaternion group; we need only check whether $\mathbf{W}$ is complemented in $\mathbf{T}$.

Now let $\mathbf{W}x$ and $\mathbf{W}y$ be two distinct elements of order 4 in $\mathbf{T}/\mathbf{W}$ that do not commute; we will have discovered such elements in obtaining more than 2 elements of order 4 in $\mathbf{T}/\mathbf{W}$. Then neither x^2 nor y^2 is in $\mathbf{W}$. We check whether $x^4 = y^4 = 1$; if not, $\mathbf{T} \neq \mathbf{Q} \times \mathbf{W}$ for any quaternion group $\mathbf{Q}$, so we may assume x and y are of order 4, and their squares are of order 2. Now if $\mathbf{T} = \mathbf{Q} \times \mathbf{W}$, $x^2 = y^2$, for the square of any element of order 4 in $\mathbf{Q} \times \mathbf{W}$ is the unique element of order 2 in $\mathbf{Q}$.

Consider $<x,y>$. If $\mathbf{T} = \mathbf{Q} \times \mathbf{W}$, every subgroup of $\mathbf{T}$ is normal, so $<x,y> = <x><y>$, of order 8 because $<x> \neq <y>$ but $<x^2> = <y^2>$. But x and y do not commute, because $\mathbf{W}x$ and $\mathbf{W}y$ don't. Thus $x^y = x^{-1}$, the only element of order 4 of the normal subgroup $<x>$ besides x. Hence $<x,y>$ is a quaternion group, and $<x,y> \cap \mathbf{W} = 1$ because its unique element of order 2, x^2, is not in **W**.

To show that we can check e) in polynomial time, we start with a lemma about finite abelian subgroups of the above-described **G**.

Lemma 1.3 Suppose **L** is a finite abelian subgroup of **G**. There is a polynomial time algorithm to obtain cyclic subgroups $\mathbf{C}_1, \mathbf{C}_2, ..., \mathbf{C}_m$ such that **L** is the direct product of the $\mathbf{C}_i$, and $|\mathbf{C}_i|$ divides $|\mathbf{C}_{i+1}|$ for $1 \leq i \leq m-1$.

Proof We modify a standard construction of such a basis for **L** [Ar, (21.1)]. First note that $|\mathbf{L}|$ divides n!, so the prime factors of $|\mathbf{L}|$ are all less than or equal to n; hence we can determine all these prime factors in polynomial time. By (ix)(a), for each p dividing $|\mathbf{L}|$ we can obtain the unique Sylow p-subgroup $\mathbf{L}_p$ of $|\mathbf{L}|$. By (xii), we obtain $\Phi(\mathbf{L}_p)$. As in the proof of Lemma 1.2, using (vii) we can get, in polynomial time, a composition series for the elementary abelian group $\mathbf{L}_p/\Phi(\mathbf{L}_p)$ that yields a set of elements $x_1, x_2, ..., x_w$ such that $\Phi(\mathbf{L}_p)<x_1, x_2, ..., x_w> = \mathbf{L}_p$, so $\mathbf{L}_p = <x_1, x_2, ..., x_w>$, and $\{x_1, x_2, ..., x_w\}$ is a minimal generating set for $\mathbf{L}_p$.

We now obtain $\mathbf{L}_p$ as the direct product of cyclic subgroups. To start, determine a generator of least order and, relabeling if necessary, call it x_1, so $|x_1| = p^k \leq |\mathbf{L}_p|$. Suppose $<x_1> \cap <x_2, ..., x_w> \neq 1$. Then there exists a positive integer s_1, a power of p with $s_1 < p^k$, such that $x_1^{s_1}$ is in $<x_2, ..., x_w>$, so there exist positive integers $s_2, ..., s_w$ such that $x_1^{s_1} x_2^{s_2} \ ... \ x_w^{s_w} = 1$. Now each $s_i = r_i q_i$, where $1 \leq r_i < p$, and q_i is a power of p, so $<x_i> = <x_i^{r_i}>$. Thus replacing each x_i by $x_i^{r_i}$ and each s_i by q_i still yields $\mathbf{L}_p = <x_1, x_2, ..., x_w>$ and $x_1^{s_1} x_2^{s_2} \ ... \ x_w^{s_w} = 1$, but now each of $s_1, s_2, ..., s_w$ is a power of p.

Obtain the smallest s_j of $s_1, s_2, ..., s_w$, and interchange x_1 and x_j if $j \neq 1$, so that $s_1 < p^k$ is the smallest of $s_1, s_2, ..., s_w$. Then s_1 divides each of $s_2, ..., s_w$, for all are powers of p. Let $k_i = s_i/s_1$ for $2 \leq i \leq w$. Then $(x_1 x_2^{k_2} \ ... \ x_w^{k_w})^{S_1} = 1$, and replacing x_1 by $x_1 x_2^{k_2} \ ... \ x_w^{k_w}$ still yields $\mathbf{L}_p = <x_1, x_2, ..., x_w>$. Now, however, $|x_1| \leq s_1 = p^j < p^k$. Note that the generating set is minimal, so $|x_1| > 1$.

Thus repeating the above process less than k times must yield a set of generators $<x_1, x_2, ..., x_w>$ such that $<x_1> \cap <x_2, ..., x_w> = 1$, so $\mathbf{L}_p = <x_1> \times <x_2, ..., x_w>$. Similarly, we break down $<x_2, ..., x_w>$ into a direct product, etc. In polynomial time, we will have $\mathbf{L}_p$ as a direct product of cyclic groups. We sort these groups (in polynomial time) so that their order increases. Hence $\mathbf{L}_p = \mathbf{P}_1 \times \mathbf{P}_2 \times ... \times \mathbf{P}_w$, where $|\mathbf{P}_i|$ divides $|\mathbf{P}_{i+1}|$ for $1 \leq i \leq w-1$, and $w < n^2$ depends on p. Then let $\mathbf{C}_m$ be the direct product of the maximal order factor $\mathbf{P}_w$ for each p dividing $|\mathbf{L}|$. Let $\mathbf{C}_{m-1}$ be the direct product of the $\mathbf{P}_{w-1}$ for each p such that $w > 1$, etc. Note that m will be the largest value of w corresponding to any p dividing $|L|$. Then it is clear that $L = C_1 \times C_2 \times \ldots \times C_m$, with $|C_i|$ dividing $|C_{i+1}|$ for $1 \le i \le m-1$ as claimed.

Proof of Theorem 1.1 Given G, let $L = G^N$, which we've seen we can obtain in polynomial time. By c) of Gaschutz' Satz 1, if L is not abelian, which we can check in polynomial time, then G is not a t-group, so we may assume that L is abelian. We use an approach inspired by Gaschutz' proof of Satz 1.

As in Lemma 1.3, decompose L into a direct product $C_1 \times C_2 \times \ldots \times C_m$ of cyclic groups, with $|C_i|$ dividing $|C_{i+1}|$ for $1 \le i \le m-1$. Let $C = \langle c_i \rangle$ for $1 \le i \le m$, and denote by e the order of C_m, which is the exponent of L. (We have already obtained these generators in the process of obtaining the P_j and C_i in Lemma 1.3.) Consider the m-1 subgroups $D_1, D_2, \ldots, D_{m-1}$, where $D_i = \langle c_i c_m \rangle$. Check by (ii) whether each of the C's and D's is normal in G. (There are less than $2n^2$ of these, so this can be done in polynomial time.) Each of the C's and D's is normal in the normal abelian group L, so is subnormal in G. Hence if any is not normal in G, G is not a t-group. Thus we may assume that all are normal. We now show that this implies that condition e) of Gaschutz' Satz 2 is satisfied.

Let x be an arbitrary element of G. Then $(C_m)^x = C_m$, so $c_m^x = c_m^r$ for some integer r. Furthermore, $(D_i)^x = D_i$ for $1 \le i \le m-1$, so $(c_i c_m)^x = (c_i c_m)^s$ for some integer s. But also $(C_i)^x = C_i$, so $c_i^x = c_i^k$ for some integer k. Hence $(c_i c_m)^x = (c_i c_m)^s = c_i^s c_m^s$, and also $(c_i c_m)^x = c_i^x c_m^x = c_i^k c_m^r$, so $c_i^s = c_i^k$ and $c_m^s = c_m^r$, because $C_i \cap C_m = 1$. This implies e divides r-s, so $|c_i|$, which divides e, divides r-s. Thus $c_i^r = c_i^s = c_i^k = c_i^x$. Therefore, for $1 \le i \le k$, $c_i^x = c_i^r$. But $L = C_1 \times C_2 \times \ldots \times C_m$, so $y^x = y^r$ for any y in L; i.e., property e) is satisfied, establishing the Theorem.

Note that Lemma 0.1 (v) and (vi) apply only to nilpotent groups. The structure constraints on solvable t-groups described above make it possible to extend that problem's solution to t-groups:

Proposition 1.4 Suppose G is a t-group.

(i) Given $B \le G$, find $N_G(B)$.

(ii) Given $B_1, B_2 \le G$, determine whether or not B_1 and B_2 are conjugate in G; and if so, find $g \in G$ such that $B_1^g = B_2$.

Note that this result is not exactly a generalization of (v) and (vi), for not all nilpotent groups are t-groups; in fact, a nilpotent group is a t-group if and only if it is a Dedekind group, for every subgroup of a nilpotent group is subnormal.

Proof (i) Suppose $|B|$ is a prime, p. If p divides $|G^N|$, then by d) of Gaschutz' Satz 1, $B \leq G^N$, so by e) of Satz 1, $N_G(B) = G$. If p doesn't divide $|G^N|$, determine the set of primes π dividing $|G/G^N|$ and obtain by (ix)(a) a Hall π- subgroup H of G containing B. Then H is a Dedekind group by a) of Satz 1, for it is isomorphic to G/G^N. Thus $H \leq N_G(B)$, and $G = HG^N$, so $N_G(B) = H\,N_{G^N}(B)$. But $[B, N_{G^N}(B)] \leq B \cap G^N = 1$, so $N_{G^N}(B) = C_{G^N}(B)$, which we can compute in polynomial time by (iv). Thus we can obtain $N_G(B) = H\,N_{G^N}(B)$ in polynomial time.

Now suppose $|B|$ is not prime. By (vii), obtain a composition series for G^N, and as in the proof of Lemma 1.2, obtain a composition series for G/G^N. Now all subgroups of G^N are normal in G, and all subgroups of G/G^N are normal in G/G^N, so combining these composition series actually yields a chief series $G = G_0 > G_1 > G_2 > \dots > G_m = 1$ for G passing through G^N, with each chief factor of prime order. The proof now proceeds exactly as that of (vi) in [KL]:

Let i be the integer such that B is a subgroup of G_i but not of G_{i+1}. Obtain $J = B \cap G_{i+1} < B$ by (iii). Suppose that in polynomial time we could compute H, where $H = N_G(J) \geq N_G(B)$, so $N_H(B) = N_G(B)$. Now $|B/J| = |B/B \cap G_{i+1}| = |BG_{i+1}/G_{i+1}|$, which equals $|G_i/G_{i+1}|$ because $|G_i/G_{i+1}|$ is prime. Now a subgroup of a t-group is a t-group [Ga], so H is a t-group, and it is easy to see that then H/J is a t-group. Thus we can compute $N_{H/J}(B/J)$ in polynomial time because B/J is of prime order. But $N_{H/J}(B/J) = N_H(B)/J$, so we can use generators of J and $N_H(B)/J$ to obtain $N_H(B) = N_G(B)$. Thus we have reduced the problem of obtaining $N_G(B)$ to that of obtaining $N_G(J)$, where $|J|$ properly divides $|B|$. Thus in a polynomial number of steps we can reduce to the case where $|B|$ is prime, establishing (i).

(ii) Suppose $B_1, B_2 \leq G$. We can check orders in polynomial time, so assume $|B_1| = |B_2|$. We know that $B_1 \cap G^N$ and $B_2 \cap G^N$ are Hall $\pi(G^N)$- subgroups of B_1 and B_2, respectively, so if B_1 and B_2 are conjugate in G, so are $B_1 \cap G^N$ and $B_2 \cap G^N$. But all subgroups of G^N are normal in G, so if B_1 and B_2 are conjugate in G, then $B_1 \cap G^N = B_2 \cap G^N$. By (iii), we can compute these two subgroups in polynomial time. Thus we may assume $B_1 \cap G^N = B_2 \cap G^N$.

Thus $|G^N B_1| = |G^N B_2|$. Now if B_1 and B_2 are conjugate in G, then $G^N B_1$ and $G^N B_2$ are conjugate in G. But these are normal in G, so they are equal. Since we can easily obtain $\mathbf{G^{\mathcal{N}}B_1}$ and $\mathbf{G^{\mathcal{N}}B_2}$ from $\mathbf{G^{\mathcal{N}}}$, $\mathbf{B_1}$, and $\mathbf{B_2}$, we may assume $\mathbf{G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$. Clearly any Hall $\pi(\mathbf{G/G^{\mathcal{N}}})$- subgroup of $\mathbf{B_1}$ or $\mathbf{B_2}$ is a Hall $\pi(\mathbf{G/G^{\mathcal{N}}})$- subgroup of $\mathbf{G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$, so these are conjugate in $\mathbf{G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$. Hence $\mathbf{B_1}$ and $\mathbf{B_2}$ are conjugate in $\mathbf{G}$ if and only if $|\mathbf{B_1}| = |\mathbf{B_2}|$ and $\mathbf{B_1 \cap G^{\mathcal{N}} = B_2 \cap G^{\mathcal{N}}}$.

Now suppose $\mathbf{B_1}$ and $\mathbf{B_2}$ are conjugate in $\mathbf{G}$. As seen above, $\mathbf{B_1 \cap G^{\mathcal{N}} = B_2 \cap G^{\mathcal{N}}}$, $\mathbf{G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$, and $\mathbf{B_1}$ and $\mathbf{B_2}$ are conjugate in $\mathbf{G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$. Thus we may assume $\mathbf{G = G^{\mathcal{N}}B_1 = G^{\mathcal{N}}B_2}$. Then let $\mathbf{D}$ be a Hall $\pi(\mathbf{G/G^{\mathcal{N}}})$- subgroup of $\mathbf{B_1}$ and $\mathbf{E}$ be a Hall $\pi(\mathbf{G/G^{\mathcal{N}}})$-subgroup of $\mathbf{B_2}$, obtainable in polynomial time by (ix)(a). Then $\mathbf{D}$ and $\mathbf{E}$ are Hall subgroups of $\mathbf{G}$. Use (ix)(b) to obtain g in $\mathbf{G}$ such that $\mathbf{D^g = E}$. But $\mathbf{B_1 = (B_1 \cap G^{\mathcal{N}})D}$ and $\mathbf{B_2 = (B_1 \cap G^{\mathcal{N}})E}$, so $\mathbf{B_1^g = B_2}$, and we are done.

2. Testing for pronormality and computing normalizers of pronormal subgroups

P. Hall showed in the 1920's that if G is a finite solvable group, then for each p in $\pi(G)$, the set of primes dividing $|G|$, G contains at least one Hall p'-subgroup [DH, I(3.3)]. For each p in $\pi(G)$, choose one such Hall p'-subgroup and denote it by $S_{p'}$. Define a function Σ from the set of all primes to the set of subgroups of G via $\Sigma(p) = S_{p'}$ if p is in $\pi(G)$ and $\Sigma(p) = G$ if not. We call this Σ a *complement system* for G. Hall proved in the 1930's that the complement systems of G are conjugate in G, where a conjugate Σ^g is defined in the obvious way by $\Sigma^g(p) = \Sigma(p)^g$ [DH, I(4.11), I(4.18)]. The system normalizer $N_G(\Sigma)$ is defined as $\{g \in G : \Sigma = \Sigma^g\}$. Clearly $N_G(\Sigma)$ is a subgroup of G. If π is any subset of the set of primes $\pi(G)$ dividing $|G|$, then the intersection of the $S_{p'}$ in Σ such that p is in $\pi(G)$-π will be a Hall π-subgroup of G. If H is a subgroup of G, we say Σ *reduces* to H if $\Sigma \cap H$, defined by $\Sigma \cap H(p) = \Sigma(p) \cap H$, is a complement system for H. Then pronormality can be characterized as follows:

> Suppose Σ is a complement system of G that reduces to U.
> Then U pr G if and only if Σ reduces to no other conjugate of U.
> [DH, I(6.6)]

It is easy to see that Σ reduces to H if and only if Σ^g reduces to H^g. Thus an equivalent characterization of pronormality is:

> Suppose Σ is a complement system of G that reduces to U.
> Then U pr G if and only if for all g such that Σ^g reduces to U, g normalizes U.

The *reducer* $R_G(H)$ is defined to be $<x \in G$: Σ^x reduces to $H>$. The remarks above imply that for all $H \leq G$, $R_G(H) \geq N_G(H)$, and that $R_G(U)=N_G(U)$ if and only if U pr G.

Note that for any $H \leq G$, any complement system for H can be obtained as $\Sigma \cap H$ for some complement system Σ of G: For each p in $\pi(H)$, the Hall p'-subgroup of H is contained in a Hall p'-subgroup of G, while for each p in $\pi(G)-\pi(H)$, H itself is contained in a Hall p'-subgroup of G. Thus for any subgroup H of G, there is some complement system Σ of G reducing to H.

A useful and easily checked fact is that if U pr G and Σ reduces to U, then the system normalizer $N_G(\Sigma)$ is contained in $N_G(U)$. For if $\Sigma = \Sigma^g$, then Σ reduces to $U^{g^{-1}}$. Thus $g^{-1} \in R_G(U) = N_G(U)$, and therefore $g \in N_G(U)$.

Carter [Ca] has studied several invariants of solvable groups and embedded subgroups, three of which are useful here. One is w(G), defined to be the number of complement systems of G. Because G acts transitively on these complement systems, $w(G) = |G:N_G(\Sigma)|$, where Σ is any one of these complement systems, and $N_G(\Sigma)$ is its stabilizer under the action of G.

Another invariant is $z_0(U)$, where $U \leq G$. Here is how Carter defines $z_0(U)$: Begin with a U-composition series $G=H_0> H_1> H_2... > H_r = 1$, so that all the H_j's are normalized by U, and for $0 < j \leq r$, H_j is normal in H_{j-1} and H_{j-1}/H_j has no nontrivial proper subgroup normalized by U. Thus $H_j(H_{j-1} \cap U)/H_j$ must be trivial or equal to H_{j-1}/H_j. In the former case, we say U *avoids* H_{j-1}/H_j; in the latter case U *covers* H_{j-1}/H_j. Also, the factor group H_{j-1}/H_j is called *central* if U centralizes it, and *eccentric* otherwise. $z_0(U)$ is defined to be the product of the orders of the central factors in that U-composition series avoided by U. Carter shows that $z_0(U)$ is independent of the choice of U-composition series for G [Ca, p.539].

Finally, Carter defines $\sigma(U)$ to be the number of complement systems of G that reduce to U, and proves:

(*) $\sigma(U) = z_0(U)w(G)/|G:U|$ [Ca, p.541].

We are now in position to prove a largely numerical criterion for pronormality:

Theorem 2.1 Suppose $U \leq G$, where G is any finite solvable group, and Σ is a complement system for G that reduces to U. Then U pr G if and only if $z_0(U) = |N_G(U):U|$, and $z_0(U) > |N_G(U):U|$ if U is not pronormal in G.

Proof If U pr G then $N_G(\Sigma) \leq N_G(U)$, and Σ^g reduces to U if and only if g is in $N_G(U)$. Thus the number of complement systems for G reducing to U, $\sigma(U)$, is $|N_G(U):N_G(\Sigma)|$. Then by (*), substituting $|G:N_G(\Sigma)|$ for $w(G)$, we have $|N_G(U):N_G(\Sigma)| = z_0(U)|G:N_G(\Sigma)|/|G:U|$, which yields $z_0(U) = |N_G(U):U|$.

Now suppose U is not pronormal in G, so some generator x of $R_G(U)$ is not in $N_G(U)$. Elements of $N_G(U)$ yield $|N_G(U):N_G(\Sigma) \cap N_G(U)|$ distinct conjugates of Σ. Suppose $N_G(\Sigma) \leq N_G(U)$. If $\Sigma^x = \Sigma^n$ for some n in $N_G(U)$, then xn^{-1} is in $N_G(\Sigma) \leq N_G(U)$, so x is in $N_G(U)$, a contradiction. Thus $\sigma(U) > |N_G(U):N_G(\Sigma) \cap N_G(U)| = |N_G(U):N_G(\Sigma)|$. If $N_G(\Sigma)$ is not contained in $N_G(U)$, $\sigma(U) \geq |N_G(U):N_G(\Sigma) \cap N_G(U)| > |N_G(U):N_G(\Sigma)|$. Hence $|N_G(U):N_G(\Sigma)| < z_0(U)w(G)/|G:U|$ by (*), and $z_0(U) > |N_G(U):U|$.

The following criterion for pronormality in a speicial case forms the inductive step below in the more general case. It exploits the link between computation of the normalizer and determination of pronormality presented in Theorem 2.1.

Lemma 2.2 Suppose X is a solvable group with subgroups N and U such that N is an elementary abelian p-group, and N and UN are normal in X. Let Σ be a complement system of X reducing to U, P be the Sylow p-subgroup of X associated with Σ, and S be the Hall p'-subgroup of X in Σ. Let $T = \langle U,S,N \cap C_{UN}(U/U \cap N),N_{UP}(\Sigma \cap UP)\rangle$. Then U pr X if and only if $T \leq N_X(U)$ and $|T:U| = z_0(U)$. Furthermore, if U pr X, then $N_X(U) = T$.

Proof Note $UP = UNP \leq X$. Also, if H is the Hall q'- subgroup in Σ for some $q \neq p$, then $P \leq H$, and $H \cap UNP = (H \cap UN)P$ is a Hall q'-subgroup of UNP because UN is normal in X. Similarly, $S \cap UNP = S \cap UN$ is a Hall p'- subgroup of UN and of UNP. Thus Σ reduces to UP; i.e., $\Sigma \cap UP$ is a complement system for UP. Denote by D the system normalizer $N_{UP}(\Sigma \cap UP)$.

Note that $U \cap N$ is normalized by U because N is normal in X, and by N because N is abelian. Thus $U \cap N$ is normal in UN. Hence $C_{UN/U \cap N}(U/U \cap N) = C/U \cap N$ for some $C \leq UN$, and $C = C_{UN}(U/U \cap N)$.

Now if $T \leq N_X(U)$ and $|T:U| = z_0(U)$, then $|N_X(U):U| \geq z_0(U)$. Thus by Theorem 2.1, U pr X.

Conversely, suppose U pr X. We show first that $T \leq N_X(U)$. Clearly $U \leq N_X(U)$. Also $C_{UN/U\cap N}(U/U\cap N) = C/U\cap N$ implies $[U,C] \leq U\cap N \leq U$, so $C \leq N_{UN}(U)$ and $N\cap C \leq N\cap N_{UN}(U)$. On the other hand, $[U,N\cap N_{UN}(U)] \leq U\cap N$, so $N\cap N_{UN}(U)$ is contained in C and therefore in $N\cap C$. Hence $N\cap C = N\cap N_{UN}(U)$. Set $L = N\cap N_{UN}(U) = N\cap N_X(U)$.

We now show $X = N_X(U)N$. UN is normal in X, so $X = N_X(UN) \geq N_X(U)N$. Let x be an arbitrary element of X. Then $U^x = U^a$ for some $a \in \langle U,U^x\rangle$ because U pr X. Hence $xa^{-1} \in N_X(U)$. But UN is normal in X, so $\langle U,U^x\rangle \leq UN$. Thus $a \in UN$, so $x \in N_X(U)UN = N_X(U)N$, and $X = N_X(U)N$, as claimed.

Now U pr X implies U pr UP, so $N_{UP}(\Sigma\cap UP) \leq N_{UP}(U) \leq N_X(U)$ [DH, I(6.8)]. Thus $D = N_{UP}(\Sigma\cap UP) \leq N_X(U)$. Also, U pr X implies Σ reduces to $N_X(U)$ [DH, I(6.8)], so $S\cap N_X(U)$ is a Hall p'-subgroup of $N_X(U)$. But $X = N_X(U)N$, where N is a p-group, so $S\cap N_X(U)$ is a Hall p'- subgroup of X; i.e., $S\cap N_X(U) = S$, so $S \leq N_X(U)$. Hence $T = \langle U,S,L,D\rangle \leq N_X(U)$.

Because Σ reduces to $N_X(U)$, $P\cap N_X(U)$ is a Sylow p- subgroup of $N_X(U)$, so $N_X(U) = \langle S,P\cap N_X(U)\rangle$. If we can show that $P\cap N_X(U) \leq \langle U,D,L\rangle \leq N_X(U)$, we will have $N_X(U) \leq \langle S,U,L,D\rangle \leq T \leq N_X(U)$, so $T = N_X(U)$, and $|T:U| = z_0(U)$ by Theorem 2.1. Thus it remains to show $P\cap N_X(U) \leq \langle U,L,D\rangle$.

Now $L = N\cap N_X(U)$, so L is normalized by $N_X(U)$ because N is normal in X and L is normalized by N because N is abelian. But $X = N_X(U)N$, so L is normal in X. Also, $L \leq UNP = UP$, so L is a normal subgroup of UP. And $N \leq UP$, so $UP = N_{UP}(U)N$. We show now that $N_X(UL) = N_X(U)$. Clearly $N_X(U) \leq N_X(UL)$, so start with $x \in N_X(UL)$. Then $\langle U,U^x\rangle \leq UL$, so there exists $a \in UL$ such that $U^x = U^a$. But $L \leq N_X(U)$, so $UL \leq N_X(U)$ and $U^a = U$; hence $x \in N_X(U)$. Thus $N_{UP}(UL) = N_{UP}(U)$ and $UP = N_{UP}(UL)N$.

Note also that U pr X implies UL pr X because L is normal in X [DH, I(6.4)].

If $E \leq UP$, denote by $\overline{E}$ the group EL/L, and denote by Ψ the complement system $(\Sigma\cap UP)L/L$ for $\overline{UP}$. First note that $N_{\overline{UP}}(\overline{UL})\cap\overline{N} = (N_{UP}(UL)\cap N)/L \leq (N_X(UL)\cap N)/L = (N_X(U)\cap N)/L = L/L = 1$. Also, $UP = N_{UP}(UL)N$ implies $\overline{UP} = N_{\overline{UP}}(\overline{UL})\overline{N}$. Thus $|N_{\overline{UP}}(\overline{UL})| = |\overline{UP}|/|\overline{N}|$.

Now $\overline{UN}$ is normal in $\overline{UP}$, with $\overline{UP}/\overline{UN}$ a p-group. And system normalizers are preserved under epimorphisms [DH, I(5.8)], so $\overline{D} = N_{\overline{UP}}(\overline{\Psi})$ and $\overline{D}\,\overline{UN}/\overline{UN}$ is a system normalizer of the nilpotent group $\overline{UP}/\overline{UN}$. But all Hall subgroups of a nilpotent group are normal, so a nilpotent group is its own system normalizer. Then $\overline{D}\,\overline{UN}/\overline{UN} = \overline{UP}/\overline{UN}$ and $\overline{UP} = \overline{D}\,\overline{UN}$, so $\langle\overline{D},\overline{U}\rangle\overline{N} = \overline{UP}$. Thus $|\langle\overline{D},\overline{U}\rangle| \geq |\overline{UP}|/|\overline{N}|$. But $\overline{U} = \overline{UL}$ pr $\overline{UP}$, because UL pr UP. Hence $\overline{D} = N_{\overline{UP}}(\overline{\Psi}) \leq N_{\overline{UP}}(\overline{UL})$. Hence $\langle\overline{D},\overline{U}\rangle \leq N_{\overline{UP}}(\overline{UL})$, whose order is $|\overline{UP}|/|\overline{N}|$. Therefore, $\langle\overline{D},\overline{U}\rangle = N_{\overline{UP}}(\overline{UL})$. Thus

$\langle DL,UL\rangle = N_{UP}(UL) = N_{UP}(U)$, so $N_{UP}(U) = \langle D,U\rangle L$. Hence $P\cap N_X(U) \le N_{UP}(U)$ implies $P\cap N_X(U) \le \langle U,L,D\rangle$, establishing the Lemma.

Now suppose $\mathbf{G} = G/K$ and $\mathbf{U} = U/K$, where K is normal in G and U and $U \le G \le \mathrm{Sym}(n)$. We will produce a polynomial-time algorithm for checking whether **U** is pronormal in **G** if **G** is solvable. In the process, we will produce a polynomial-time method for obtaining the normalizer of **U** if it is indeed pronormal in **G**. As mentioned above, in [Lu2], Luks presents a polynomial-time method for computing the normalizer of any subgroup of **G** [Lu2, Corollary 3.3]. To obtain this result for arbitrary subgroups, he develops more complex machinery than is used here for the special case of pronormal subgroups [Lu2, Section 6].

Theorem 2.3 If **U** and **G** are as described above, there is a polynomial time algorithm to determine whether **U** is pronormal in **G**, and if so, compute $N_{\mathbf{G}}(\mathbf{U})$.

Proof We proceed recursively, keeping track of $c(\mathbf{G})$, the number of prime factors, counting multiplicities, in the prime factorization of $|\mathbf{G}|$. $G \le \mathrm{Sym}(n)$, so $c(\mathbf{G}) \le c(G) \le \log(n!) \le n\log n$. Thus the number of recursive steps using $c(\mathbf{G})$ will be polynomially bounded.

Using (viii)(a), obtain a minimal normal subgroup **N** of **G**. We know that if **U** is pronormal in **G**, then **UN** is pronormal in **G** [DH, I(6.4)]. Recursively consider the subgroup **UN/N** of **G/N**, where $c(\mathbf{G/N}) < c(\mathbf{G})$. If **UN/N** is not pronormal in **G/N**, then **UN** is not pronormal in **G**, so **U** is not pronormal in **G**, and we are done. If **UN/N** is pronormal in **G/N**, we compute $N_{\mathbf{G/N}}(\mathbf{UN/N}) = N_{\mathbf{G}}(\mathbf{UN})/\mathbf{N}$ in polynomial time, easily yielding $N_{\mathbf{G}}(\mathbf{UN})$. Note that **UN/N** pr **G/N** implies **UN** pr **G**.

Now let $\mathbf{X} = N_{\mathbf{G}}(\mathbf{UN})$. We can obtain, in polynomial time, Hall p'-subgroups of **U**, and therefore a complement system for **U**, and then, again in polynomial time, obtain Hall p'-subgroups of **X** containing the elements of this complement system for **U** [KT, (5.5); (ix)(a)]. Thus we can obtain in polynomial time a complement system Σ for **X** that reduces to **U**. Note that **UN** is normal in $\mathbf{X} = N_{\mathbf{G}}(\mathbf{UN})$, so we can use Lemma 2.2. Now we check that we can compute $\mathbf{T} = \langle \mathbf{U},\mathbf{S},\mathbf{N}\cap C_{\mathbf{UN}}(\mathbf{U}/\mathbf{U}\cap\mathbf{N}), N_{\mathbf{UP}}(\Sigma\cap\mathbf{UP})\rangle$ in polynomial time. We have **U** of course, and we already have **S** as part of our complement system Σ. Because **X** is solvable, we can compute $\mathbf{U}\cap\mathbf{N}$, then compute $\mathbf{C}/\mathbf{U}\cap\mathbf{N} = C_{\mathbf{UN}}(\mathbf{U}/\mathbf{U}\cap\mathbf{N})$ by (iv). Thus we can obtain **C** and $\mathbf{N}\cap\mathbf{C}$.

Finally, **P** is the intersection of the Hall q'- subgroups of Σ such that $q \neq p$, which we can obtain in polynomial time by (iii), so we can get **UP**. We can intersect **UP** with each of the elements of Σ to obtain $\Sigma \cap \mathbf{UP}$. But $N_{\mathbf{UP}}(\Sigma \cap \mathbf{UP})$ is the intersection of the normalizers of at most n known Hall p'-subgroups of **UP**, for each prime p dividing $|G| = n!$ is less than or equal to n. Thus we can obtain generators for these normalizers in polynomial time by (ix)(c) and compute their intersection $N_{\mathbf{UP}}(\Sigma \cap \mathbf{UP})$ in polynomial time as well. Hence we can obtain **T** in polynomial time, and use (i) to get $|\mathbf{T}|$ and $|\mathbf{U}|$, so we can compute $|\mathbf{T}:\mathbf{U}|$.

Now $\mathbf{T} \leq N_{\mathbf{X}}(\mathbf{U})$ if and only if $<\mathbf{U},\mathbf{U}^{t}> = \mathbf{U}$ for each of the generators we have obtained for **T**, and we can check this in polynomial time by (i). If **T** is not contained in $N_{\mathbf{X}}(\mathbf{U})$, then **U** is not pronormal in **X**, so it is not pronormal in **G**, and we are done. So suppose $\mathbf{T} \leq N_{\mathbf{X}}(\mathbf{U})$. Then by Lemma 2.2, **U** pr **X** if and only if $|\mathbf{T}:\mathbf{U}| = z_0(\mathbf{U})$, so it remains to compute $z_0(\mathbf{U})$ in polynomial time.

Next, we construct a **U**-composition series for **X** passing through $\mathbf{U} \cap \mathbf{N}$, **N**, and **UN**. Although it is not necessary to constuct the entire **U**-composition series to compute $z_0(\mathbf{U})$, it seems worthwhile to demonstrate that this can be done in polynomial time.

Note first that $\mathbf{U} \cap \mathbf{N}$ is elementary abelian of order p^d for some prime, p, and positive integer, d. Consider $\mathbf{U} \cap \mathbf{N}$ as a vector space of dimension d over the field F of p elements. Clearly $p^d \leq n! \leq n^n$, so $d \leq n^2$. Obtain a set of generators for **U** of size less than n^2 [Lu1, p.9]; this yields a set of generators for $\mathbf{U} = U/K$ of size $< n^2$. By [Ro, p.372], in polynomial time we can obtain a basis for $\mathbf{U} \cap \mathbf{N}$ over F and express each generator as a dxd matrix with entries in F. Consider the algebra J over F generated by these matrices. Then by [Ro, p.371], we can obtain a minimal J-invariant subspace **W** of $\mathbf{U} \cap \mathbf{N}$, which is a minimal **U**-invariant subgroup of $\mathbf{U} \cap \mathbf{N}$, in time that is polynomial in n. Apply this process to the vector space $\mathbf{U} \cap \mathbf{N}/\mathbf{W}$, etc. Repeating the process at most d times yields the terms of a **U**-composition series $1 = \mathbf{N}_t < \mathbf{N}_{t-1} \ldots < \mathbf{N}_{j-1} < \mathbf{N}_j = \mathbf{U} \cap \mathbf{N}$ for $\mathbf{U} \cap \mathbf{N}$.

We can do the same thing for the vector space $\mathbf{N}/\mathbf{U} \cap \mathbf{N}$, obtaining a **U**-composition series $\mathbf{U} \cap \mathbf{N}/\mathbf{U} \cap \mathbf{N} = \mathbf{N}_j/\mathbf{U} \cap \mathbf{N} < \mathbf{N}_{j-1}/\mathbf{U} \cap \mathbf{N} \ldots < \mathbf{N}_1/\mathbf{U} \cap \mathbf{N} < \mathbf{N}_0/\mathbf{U} \cap \mathbf{N} = \mathbf{N}/\mathbf{U} \cap \mathbf{N}$ for $\mathbf{U}/\mathbf{U} \cap \mathbf{N}$. Clearly $\mathbf{N}_i$ and $\mathbf{N}_{i-1}$ are consecutive terms in a **U**-composition series for any i, $1 \leq i \leq j$. For if $\mathbf{N}_i < \mathbf{M} < \mathbf{N}_{i-1}$, for some **U**-invariant subgroup **M** of **N**, $\mathbf{N}_i/\mathbf{U} \cap \mathbf{N} < \mathbf{M}/\mathbf{U} \cap \mathbf{N} < \mathbf{N}_{i-1}/\mathbf{U} \cap \mathbf{N}$, where $\mathbf{M}/\mathbf{U} \cap \mathbf{N}$ is **U**-invariant. This is impossible, because $\mathbf{N}_i/\mathbf{U} \cap \mathbf{N}$ and $\mathbf{N}_{i-1}/\mathbf{U} \cap \mathbf{N}$ are consecutive terms of a **U**-composition series for $\mathbf{N}/\mathbf{U} \cap \mathbf{N}$. Next, obtain a chief series $\mathbf{U} \cap \mathbf{N}/\mathbf{U} \cap \mathbf{N} = \mathbf{U}_s/\mathbf{U} \cap \mathbf{N} < \mathbf{U}_{s-1}/\mathbf{U} \cap \mathbf{N} \ldots < \mathbf{U}_1/\mathbf{U} \cap \mathbf{N} < \mathbf{U}_0/\mathbf{U} \cap \mathbf{N} = \mathbf{U}/\mathbf{U} \cap \mathbf{N}$ for $\mathbf{U}/\mathbf{U} \cap \mathbf{N}$ by (viii)(b).

Now for $0 \leq i \leq s$, $N \cap U_i = U \cap N$, so $|NU_i| = |N||U_i|/|N \cap U_i| = |N||U_i|/|U \cap N|$, and $N = NU_s < NU_{s-1} \ldots < NU_1 < NU_0 = NU = UN$. Suppose $NU_i < M < NU_{i-1}$ and M is U-invariant. Then $M \geq N$ implies $M = N(M \cap U_{i-1})$, and $(M \cap U_{i-1}) \cap N = M \cap U \cap N = U \cap N$. Hence $|M| = |N||M \cap U_{i-1}|/|U \cap N|$, so $|U_i| < |M \cap U_{i-1}| < |U_{i-1}|$. Thus $M \cap U_{i-1}$ is a U-invariant (i.e. normal) subgroup of U strictly between U_i and U_{i-1}, so $M \cap U_{i-1}/U \cap N$ is a U-invariant subgroup of $U/U \cap N$ that is strictly between $U_i/U \cap N$ and $U_{i-1}/U \cap N$, which is impossible, because these subgroups are consecutive terms of a chief series for $U/U \cap N$. Hence NU_i and NU_{i-1} are legitimate consecutive terms in a U-composition series for X. Thus $1 = N_t < N_{t-1} \ldots < N_1 < N_0 < NU_{s-1} \ldots < NU_0 = UN$ is a U-composition series for UN. We need only obtain the terms of the series above the normal subgroup UN.

But that is easy, because $U \leq UN$: Simply obtain a composition series for X/UN by (vii) and use these terms' preimages in G to get $UN = V_r < V_{r-1} \ldots < V_1 < V_0 = X$. Each V_i is U-invariant because it contains U, and V_{i-1}/V_i is of prime order, so these terms do indeed complete our U-composition series for X.

Now note that U avoids each of the composition factors of the form V_{i-1}/V_i, for $V_{i-1} \cap U = V_i \cap U = U$. Furthermore, each of these is a central factor, for $[V_{i-1}/N, UN/N] \leq UN/N$, a normal subgroup of G/N. Hence $[V_{i-1}, U] \leq UN \leq V_i$, so U centralizes V_{i-1}/V_i. Thus in computing Carter's $z_0(U)$, we must include the product of all these V_{i-1}/V_i 's, which is |G:UN|. Clearly U covers the NU_{i-1}/NU_i 's, and the terms below $U \cap N$, but it does avoid the N_{i-1}/N_i's for $1 \leq i \leq j$. Thus it is necessary to check which among the polynomially bounded number of factors of the form N_{i-1}/N_i are centralized by every one of the less than n^2 generators of U; clearly this can be done in polynomial time. Alternatively, we can invoke (iv) and check for each i whether $C_{UN/N_i}(N_{i-1} / N_i) = UN/N_i$.

Thus we can compute $z_0(U)$ in X in polynomial time. Now check whether $|T:U| = z_0(U)$ and apply Theorem 2.1. If $|T:U| \neq z_0(U)$, U is not pronormal in X or G, so we are done. If $|T:U| = z_0(U)$, U is pronormal in X.

By Lemma 2.2, if U is pronormal in X, then $N_X(U) = T$, which we can construct in polynomial time. But $X = N_G(UN)$, so X contains $N_G(U)$. Hence $N_G(U) = N_X(U)$. Now that we have $N_G(U)$, we could use Theorem 2.1 to check whether U is pronormal in G, but there is an easier way. For U pr $N_G(UN)$ and UN pr G implies U pr G [DH, I(6.4)], so since $X = N_G(UN)$, U is indeed pronormal in G, and we are done.

Acknowledgements The author wishes to thank Eugene Luks of the University of Oregon Computer and Information Science Department and Gary Seitz and Charles

Wright of the University of Oregon Mathematics Department for valuable conversations regarding this report.

References

[Ar] M. A. Armstrong, Groups and Symmetry, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo 1988.

[Ca] R.W. Carter, *Nilpotent Self-Normalizing Subgroups and System Normalizers*, London J. Math. 12 (1962) 535-563.

[DH] K. Doerk and T. Hawkes, Finite Soluble Groups, de Gruyter, Berlin and New York 1992.

[Fe] A. Feldman, *t-groups and their generalizations*, (to appear in Proceedings of the Ohio State Denison Conference in memory of Hans Zassenhaus).

[Ha] M. Hall, Jr., The Theory of Groups, Macmillan, New York and Toronto 1959.

[KL] W.M. Kantor and E.M. Luks, Computing in Quotient Groups, Dept. of Comp. and Info. Sci., U. of Oregon (1990).

[KT] W.M. Kantor and D.E. Taylor, *Polynomial-Time Versions of Sylow's Theorem*, J. of Algorithms 9 (1988) 1-17.

[Lu1] E.M. Luks, Lectures on Polynomial-time Computation in Groups, Dept. of Comp. and Info. Sci., U. of Oregon (1990).

[Lu2] E.M. Luks, Computing in Solvable Matrix Groups, Dept. of Comp. and Info. Sci., U. or Oregon (1992).

[Ro] L. Ronyai, *Computing the Structure of Finite Algebras*, J. Symbolic Computation 9 (1990) 355-373.