Existence of Hall Subgroups and Embedding of \( \pi \)-Subgroups into Hall Subgroups*

PHILIP COBB

Mathematics Department, Texas A & M University,
College Station, Texas 77843

Communicated by Walter Feit
Received April 21, 1988

1. INTRODUCTION

The investigation of the arithmetic structure of finite groups begins with Sylow's Theorem. A generalization of Sylow subgroups involving more than one prime was introduced in 1928 by Philip Hall. Let \( \pi \) be a set of primes; a Hall \( \pi \)-subgroup of a finite group \( G \) is a subgroup \( H \) whose order is divisible only by primes in \( \pi \) and whose index \( [G : H] \) is not divisible by any primes in \( \pi \). More generally, a \( \pi \)-subgroup is any subgroup such that the primes dividing its order are all in \( \pi \). To study these subgroups, we will use Hall's original notation [5]: A group is said to satisfy \( E_\pi \) if there exists a Hall \( \pi \)-subgroup; it satisfies \( C_\pi \) if it satisfies \( E_\pi \) and any two Hall subgroups are conjugate; it satisfies \( D_\pi \) if it satisfies \( C_\pi \) and in addition any \( \pi \)-subgroup is contained in some Hall \( \pi \)-subgroup. Also, we use abbreviations such as \( E_\pi \) for \( E_\pi \) if \( \pi = \{ p \} \) and \( C_{\pi,r} \) for \( C_\pi \) if \( \pi = \{ p, r \} \).

In this notation, Sylow's Theorem asserts that any group satisfies \( D_p \) for any prime \( p \) and Hall's Theorem says that any solvable group satisfies \( D_\pi \) for any \( \pi \). But a non-solvable group can fail to satisfy \( E_\pi \), or may satisfy \( E_\pi \) but not \( C_\pi \), or even \( C_\pi \) but not \( D_\pi \). It had been conjectured by Hall [5] that if \( 2 \notin \pi \), then \( E_\pi \) implies \( D_\pi \). However, only half of this statement is actually true; if \( \pi \) is a set of odd primes, then \( E_\pi \) implies \( C_\pi \) but not \( D_\pi \) [3]. Counterexamples to this conjecture will be given here; some of them were independently found by Fletcher Gross [4].

Now let \( p \) be a prime number. For a group \( G \), let \( |G| \) denote its order and \( |G|_p \) be the highest power of \( p \) dividing \( |G| \), i.e., the order of its Sylow

* This paper contains portions of my Ph.D. thesis at the University of Illinois. I thank my thesis advisor, Professor Michio Suzuki, for suggesting this topic and for his help and suggestions.
If $n$ is an integer, similarly define $|n|_p$ to be the highest power of $p$ dividing $n$. We will also write $p^c | n$ if $|n|_p = p^c$.

Define the general linear group to be the group of all $n \times n$ matrices over a field of $q$ elements, denoted $GL(n, q)$, with $q$ a power of the field characteristic $p$. If we wish to emphasize the vector space on which $GL(n, q)$ acts, we may also write $GL(U)$, where $U$ is a vector space of dimension $n$. Also let $F_q$ be the field of $q$ elements and let $F_q^\times$ be its multiplicative group of non-zero elements. The following (non-standard) notation will be used throughout this paper.

**Notation 1.1.** Let $p$ be a prime and let $q$ be a power of $p$. Let $r$ and $s$ be two odd primes, different from $p$, with $r < s$. Define $a$ and $b$ to be the least positive integers so that $r | q^a - 1$ and $s | q^b - 1$. Note that $a | r - 1$ and $b | s - 1$ by Fermat's Theorem. The order of the Sylow $r$-subgroup and its construction were determined by Weir \[8].

**Lemma 1.2 (Weir).** The order of the Sylow $r$- and $s$-subgroups of $GL(n, q)$ is given by

$$|GL(n, q)|_r = |(q - 1)(q^2 - 1) \cdots (q^n - 1)|_r = q^a - 1 |^{[n/a]} |[n/a]!|_r;$$

$$|GL(n, q)|_s = |q^b - 1 |^{[n/b]} |[n/b]!|_s.$$ 

Necessary and sufficient conditions for $E_{r,s}$ in $GL(n, q)$, given numerically in terms of $a$, $b$, $r$, $s$, and $n$, were found by E. L. Spitznagel in \[6\. Section 2 of this paper will determine when $E_{r,s}$ holds in $GL(n, q)$ if $2$, $p \not\equiv \pi$. This will give counterexamples to Hall's conjecture.

Let $H$ be a subgroup of $GL(n, q)$ acting on an $n$-dimensional vector space $V$. Then $H$ acts irreducibly if it leaves no proper non-trivial subspace invariant. If $H$ is irreducible and $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$, where $k > 1$ and with the action of $H$ preserving this decomposition (but permuting the $W_i$'s), then $H$ is said to be imprimitive. The direct sum decomposition is a system of imprimitivity. If $H$ is irreducible but not imprimitive then $H$ is said to be primitive. The proofs below divide into three cases according as $H$ is reducible, irreducible but imprimitive, or primitive. For the primitive case, we need a result of Suprunenko \[7\. To facilitate the discussion, we introduce the following concepts.

**Definition 1.3.** A subgroup $G$ of $GL(n, q)$ is said to be of type $\mathcal{G}$ if there exist a divisor $d$ of $n$ and a normal series

$$F \triangleleft A \triangleleft V \triangleleft G$$

with the following properties:
(1) $F$ is isomorphic to the multiplicative group $F_{q^d}^*$ of $F_{q^d}$ and $F < G$; 
(2) $V = C_{cl}(F)$ is isomorphic to a subgroup of $GL(n/d, q^d)$; 
(3) $A$ is such that $A/F$ is the maximal normal abelian subgroup of $V/F$ and is elementary abelian of order $(n/d)^2$; 
(4) If
\[
\frac{n}{d} = t_1^{t_1} t_2^{t_2} \cdots t_k^{t_k}
\]
is the canonical primary decomposition of $n/d$, then $V/A$ is isomorphic to a subgroup of
\[
Sp(2j_1, t_1) \times \cdots \times Sp(2j_k, t_k),
\]
and
(5) $G/V$ is isomorphic to a subgroup of $Gal(F_{q^d}/F_q)$.

We will call $d$ the field degree of the group $G$ of type $\mathcal{F}$.

In this notation, Suprunenko's Theorem states

**Theorem 1.4 (Suprunenko).** Any primitive solvable subgroup $X$ of $GL(n, q)$ is contained in a group of type $\mathcal{F}$.

We will want to apply the series $F < A < V < G$ to possibly imprimitive groups. Therefore, we will make the following definition.

**Definition 1.5.** An $(r, s)$-group $L$ is of type $\mathcal{P}$ if it is contained in a group of type $\mathcal{F}$ with field degree $d$ such that

(1) $n = d$, $n/d$ is divisible by $r$, or $n/d$ is divisible by $s$ and
(2) One of $a$ or $b$ divides $d$.

By Lemma 11 in [7], we also have

**Theorem 1.6.** Any primitive $(r, s)$-subgroup of $GL(n, q)$ is of type $\mathcal{P}$.

Suppose that $G$ is of type $\mathcal{F}$. To prove that $D_x$ holds, we will need to show that the indices $[A : F]$, $[V : A]$, and $[G : V]$ in the series $F < A < V < G$ are all prime to $s$. This is handled by the following lemma.

**Lemma 1.7.** Let $s$ be a prime and let $G$ be a subgroup of $GL(n, q)$ of type $\mathcal{F}$ with field degree $d$. If $n/d < s$, then one of the following holds:

(1) The index $[V : F]$ is prime to $s$. If also $d$ is prime to $s$, then $[G : F]$ is prime to $s$; or
(2) \( n/d = 2^j \) and \( s = 2^j + 1 \) for some \( j \). In this case, \( s \) divides \( [V:F] \) only to the first power. If we also have \( d < s \), then \( [G:F] \) is divisible by \( s \) only to the first power.

In particular, if \( s > n + 1 \), then \( [G:F] \) is prime to \( s \).

Proof. By Definition 1.3, \( [A:F] = (n/d)^2 \) and \( n/d < s \) by hypothesis. This shows that \( [A:F] \) is prime to \( s \). Now consider the index \( [G:V] \). Since the factor group \( G/V \) embeds in a Galois group of order \( d \), \( [G:V] \) is prime to \( s \) if \( d \) is prime to \( s \).

Now consider the index \( [V:A] \). We have an embedding of \( V/A \) into a direct product of symplectic groups \( Sp(2j, t) \), where \( t \) is a prime and \( t^j \|(n/d) \). The order of the symplectic group is

\[
|Sp(2j, t)| = t^d(t^2 - 1)(t^4 - 1) \cdots (t^{2j} - 1) \\
= t^d(t - 1)(t + 1)(t^2 - 1)(t^2 + 1) \cdots (t^j - 1)(t^j + 1). \tag{1}
\]

We now attempt to show that each factor in the second line of (1) is prime to \( s \). Since \( t \parallel (n/d) \) and \( n/d < s \), \( t \) and \( s \) are distinct primes and \( t^j \) is prime to \( s \). Since all other factors are at most \( t^j + 1 \), it suffices to show that \( t^j + 1 < s \).

Now

\[
t^j + 1 \leq \frac{n}{d} + 1 \leq s, \tag{2}
\]

where the first inequality follows from \( t^j \|(n/d) \) and the second inequality is by assumption. If either inequality in (2) is strict, then \( t^j + 1 < s \) as required. If, however, equality holds throughout then \( t^j = n/d \) and \( s = t^j + 1 \). Since \( s \) is odd and \( t \) is prime, \( t = 2 \) and \( s = 2^j + 1 \). Since the factor \( t^j + 1 \) occurs only once in the factorization of \( |Sp(2j, t)| \), \( s \) divides \( |Sp(2j, t)| \) only to the first power. Thus either \( [V:A] \) is prime to \( s \) or \( s = 2^j + 1 = (n/d) + 1 \) and \( [V:A]_s = s \).

By the first paragraph of this proof, \( [A:F] \) is prime to \( s \) and \( [G:V] \) is prime to \( s \) if \( d \) is prime to \( s \). Since

\[
[G:F] = [G:V][V:A][A:F],
\]

all the conditions in (1) are satisfied if \( [V:A] \) is prime to \( s \). If, however, \( [V:A] \) is divisible by \( s \), then all the statements in (2) hold.

There now only remains to prove the last statement. Assume that \( s > n + 1 \). Then \( (n/d) + 1 \leq n + 1 < s \). Also, \( d \) is a divisor of \( n \), so \( d < s \) is prime to \( s \). Hence either (1) or (2) holds. However, (2) implies that \( s = n + 1 \), contrary to the hypothesis that \( s > n + 1 \). Therefore, (1) must be true. Since \( d \) is prime to \( s \), \( [G:F] \) is prime to \( s \). This completes the proof.
Another useful fact is the following lemma of Hall [5]:

**Lemma 1.8 (Hall).** Let $G$ be a finite group and $N$ a normal subgroup of $G$. If $H$ is a Hall $\pi$-subgroup of $G$, then $H \cap N$ is a Hall $\pi$-subgroup of $N$ and $HN/N$ is a Hall $\pi$-subgroup of $G/N$.

2. $E_\pi$ in $GL(n, q)$

Consider the general linear group $GL(n, q)$ and assume that all the notation is as in 1.1. In this section, we will first recall the conditions for $E_{r,s}$ and the construction of Hall subgroups, which were determined in [6]. Then we will generalize the theorems on $E_\pi$ to the case where $\pi$ may contain any number of odd primes other than $p$.

In order to describe the Hall subgroups, we will need an embedding (which may also be found in [6]) of $F_q^a$ into $GL(a, q)$. Let $F = F_q$ and $K = F_q^{a_i}$. Then $K$ is the splitting field of a certain irreducible polynomial $f(x)$ of degree $a$ with coefficients in $F$. Let $\xi \in K$ be a root of $f(x)$. Then $K$ can be regarded as a vector space over $F$ with basis $1, \xi, \xi^2, ..., \xi^{a-1}$. Multiplication by an element of $K$ is an $F$-linear transformation of $K$. This transformation can be represented as a matrix with respect to the basis $\{1, \xi, \xi^2, ..., \xi^{a-1}\}$. As the non-zero elements of $K$ are invertible, they will be embedded into $GL(a, q)$.

We will now quote Spitznagel's conditions for $E_{r,s}$ in $GL(n, q)$, given in [6]. Recall the notation in 1.1; $r$ and $s$ are two odd primes neither of which is the field characteristic $p$, $r < s$, and $a$ and $b$ are the orders of $q$ modulo $r$ and $s$, respectively.

**Theorem 2.1 (Spitznagel).** Let $r$, $s$, $a$, and $b$ be as in 1.1. Then $E_{r,s}$ holds in $GL(n, q)$ if and only if one of the following three sets of conditions is true:

I. $a = b$ and $n < as$.

II. $a = r - 1$, $b = 1$, $n < bs$, $[n/a] = [n/r]$, and $|q^a - 1|, = r$.

III. $a = r - 1$, $b = r$, $n < bs$, $[n/a] = [n/r]$, and $|q^a - 1|, = r$.

In Cases II and III, we must also have $n < ar$. For $n/a - n/r = n/(r - 1) - n/r = n(1/(r - 1) - 1/r)$, an increasing function of $n$, so once $n$ exceeds $ar$, $n/a - n/r \geq ar/a - ar/r = r - a = 1$. Thus $[n/a] - [n/r] \geq 1$ if $n \geq ar$. Hence $n < ar$ in Cases II and III.

The Hall subgroups constructed in [6] are as follows:

I. Here $a = b$. Let $k = [n/a]$, and consider the group $GL(k, q^a)$. We will construct a Hall subgroup of $GL(k, q^a)$ first. Consider the subgroup $D$ of diagonal matrices of order $(q^a - 1)^k$. Take a Hall $\{r, s\}$-subgroup $H_0$ of
The group \( P \) of permutation matrices normalizes \( D \) and hence \( H_0 \). Since \( n < as \), \(|P|\) is prime to \( s \). Then let \( R \) be a Sylow \( r \)-subgroup of \( P \), which therefore normalizes \( H_0 \). Thus \( H = H_0 R \) forms a group of order

\[
|H_0| \cdot |R| = |q^a - 1|_{r,s} |k!|_r = |GL(k, q^a)|_{r,s},
\]

the second equality coming from Lemma 1.2. Thus \( H \) is a Hall \( \{r, s\} \)-subgroup of \( GL(k, q^a) \).

To obtain a Hall subgroup of \( GL(n, q) \) we proceed as follows. The group \( H \) described above consists of monomial matrices with entries from \( F_q^x \). If \( x \in F_q^x \) is one such entry, we may represent \( x \) as a matrix in \( GL(a, q) \) as described above. By replacing all entries of \( H \) in this manner, we may regard \( H \) as a subgroup of \( GL(a[n/a], q) \). By taking a direct product with an \((n-a[n/a])\)-dimensional identity matrix, we may consider \( H \) to be a subgroup of \( GL(n, q) \). Since

\[
|GL(k, q^a)|_r = |q^a - 1|_r |k!|_r = |GL(n, q)|_r,
\]

and similarly for \( s \), \( H \) is a Hall subgroup of \( GL(n, q) \).

II. Since \( a \neq b \) and \( b = 1 \), we can form a Sylow \( s \)-subgroup \( S \) of diagonal matrices. A Sylow \( r \)-subgroup \( R \) will consist of a Sylow \( r \)-subgroup of permutation matrices. Since permutation matrices normalize diagonal matrices, \( H = RS \) forms a Hall \( \{r, s\} \)-subgroup of \( GL(n, q) \).

III. Here \( b = r \). Let \( S \) be the image of a Sylow \( s \)-subgroup of \( F_q^x \) under the embedding \( F_q^x \subset GL(r, q) \). Choose an element \( \alpha \) of order \( r \) from Gal\((F_q/F_q)\). Then \( \alpha \) is an \( F_q \)-linear transformation of \( F_q \). With respect to the basis \( \{1, \zeta, \zeta^2, \ldots, \zeta^{r-1}\} \), \( \alpha \) corresponds to an \( r \) by \( r \) matrix \( A \). Since \( A \) normalizes \( S \), \( S \langle A \rangle \) is a Hall \( \{r, s\} \)-subgroup of \( GL(n, q) \). Embed \([n/r]\) copies of this group down the main diagonal to form the Hall \( \{r, s\} \)-subgroup.

Now let \( \pi \) be an arbitrary set of odd primes, none of them \( p \). We will now see when \( E_\pi \) holds, generalizing the two prime case in Theorem 2.1.

**Theorem 2.2.** Let \( \pi \) be a set of odd primes with \( p \notin \pi \) and \( r < s \) the least two, and let \( t \) be any prime in \( \pi \) with \( t \neq r \). Define \( a \) and \( b \) as in 1.1, and define \( c \) analogously (i.e., \( c \) is the order of \( q \) mod \( t \)). Then \( GL(n, q) \) satisfies \( E_\pi \) if and only if \( c = b \) for all \( t \) and one of the following holds:

I. \( a = b \) and \( n < as \);

II. \( a = r - 1, b = 1, n < bs, [n/a] = [n/r] \), and \( |q^a - 1|_r = r \);

III. \( a = r - 1, b = r, n < bs, [n/a] = [n/r] \), and \( |q^a - 1|_r = r \).

**Proof.** Assume that \( GL(n, q) \) satisfies \( E_\pi \). By the Feit–Thompson and
Hall Theorems, $E_{r,s}$ holds. By Theorem 2.1, one of the sets of conditions I, II, or III is true.

We now show that $c = b$ for all primes $t \in \pi$ with $t > r$. If $t = s$, then trivially $c = b$, so assume that $t \neq s$. By the Feit-Thompson and Hall Theorems, $E_{r,s}$, $E_{r,t}$, and $E_{s,t}$ all hold for every $t$. Assume (for a contradiction) that $b \neq c$ and thus II or III holds for $(s, t)$. In particular, $b = s - 1$ is even. If II or III should hold for $(r, s)$, then we would have $b = 1$ or $b = r$, contradicting the fact that $s$ is odd. Hence I holds for $(r, s)$ and $a = b = s - 1$. This is a contradiction, since $a < r - 1 < s - 1$. Hence I holds for $(s, t)$ and $b = c$, as desired.

Conversely, assume that I, II, or III holds. Begin by supposing that all the conditions of I are satisfied. In this case, first form a Hall $\pi$-subgroup $H_0$ of $F_q^\times$ (as embedded in $GL(a, q)$). Construct $H_1$ by placing $[n/a]$ copies of $H_0$ down the main diagonal, together with a complementary identity matrix. Then choose a Sylow $r$-subgroup $R$ of permutation matrices on $a$ by $a$ blocks, isomorphic to a Sylow $r$-subgroup of $\Sigma_{[n/a]}$. Let $H = H_0 R$. Then

$$|H| = |q^a - 1|^{[n/a]} |\Sigma_{[n/a]}| = |GL(n, q)|_r,$$

and $|H| = |q^a - 1|^{[n/a]} = |GL(n, q)|_r$, since $n < as < at$ and $[n/a] < t$.

If II holds, we may take a Hall $\pi - \{r\}$-subgroup of $F_q^\times$ and embed $n$ copies of it diagonally into $GL(n, q)$. Let $H$ be the group generated by a Sylow $r$-subgroup of the permutation matrices and a subgroup of (normal) diagonal matrices. This is a Hall $\pi$-subgroup since

$$|GL(n, q)|_r = |q^a - 1|^{[n/a]} |\Sigma_{[n/a]}| = r^{[n/a]} = r^{[n/r]} = |H|,$$

since $n < ar$, as in the two prime case. Also,

$$|GL(n, q)|_t = |q^b - 1|^{[n/b]} |\Sigma_{[n/b]}| = |q - 1|^n = |H|.$$

If III holds, then embed $F_q^\times$ into $GL(b, q)$. Since the extension has degree $r$ its Galois group, $Gal(F_q^\times / F_q)$, has an element of order $r$. This normalizes $F_q^\times$, where both are in matrix form, just as when $\pi$ had two primes. Thus the two form a solvable group. By Hall’s Theorem, this has a Hall $\pi$-subgroup. Embed $[n/b]$ copies of it in $GL(n, q)$ down the main diagonal. Call this group $H$. Then

$$|GL(n, q)|_r = |q^a - 1|^{[n/a]} |\Sigma_{[n/a]}| = r^{[n/a]} = r^{[n/r]} = r^{[n/b]} = |H|,$$

$$|GL(n, q)|_t = |q^b - 1|^{[n/b]} |\Sigma_{[n/b]}| = |q - 1|^b = |H|,$$

so we have a Hall $\pi$-subgroup in this case also.
3. $D_{r,s}$ in $GL(n, q)$

Now, turn to the question of $D_{r,s}$. First consider Case II.

**Theorem 3.1.** Let $r$ and $s$ be odd primes dividing the order of $GL(n, q)$. Assume the conditions for $E_{r,s}$ in Case II of Theorem 2.1. Then $D_{r,s}$ does not hold.

**Proof.** Since $r \mid |GL(n, q)|$ we have $n \geq a$. Suppose that $n = a$. Then since $a = r - 1$,

$$0 = \left[ \frac{a}{a + 1} \right] = \left[ \frac{a}{r} \right] = \left[ \frac{a}{a} \right] = 1,$$

a contradiction. Then $n > a$, i.e., $n \geq r$.

Let $U$ be an $n$-dimensional space of column vectors over $F_q$ on which $GL(n, q)$ acts naturally. Let $\{e_1, \ldots, e_n\}$ be the usual basis for $U$. Let $m = \lfloor n/r \rfloor$ and $c = n - rm$. Decompose $U$ as a direct sum

$$U = U_1 \oplus U_2 \oplus \cdots \oplus U_m \oplus W,$$

where each $U_i = \langle e_{(i-1)r+1}, \ldots, e_{ir} \rangle$ is an $r$-dimensional subspace and $W = \langle e_{mr+1}, \ldots, e_n \rangle$ is a subspace of dimension $n - rm$. Let $H$ be the Hall subgroup constructed in Theorem 2.1. We will now describe the Sylow $r$- and $s$-subgroups of $H$ as they act on $U$. Let $R_i$ be a group, acting on $U_i$, generated by a permutation matrix of order $r$. The Sylow $r$-subgroup $R$ of $H$ is then

$$R = R_1 \times R_2 \times \cdots \times R_m.$$

Since $b = 1$, $GL(n, q)$ has a Sylow $s$-subgroup $S$ of diagonal matrices. Let $H = \langle R, S \rangle$. By construction, each $U_i$ is an irreducible subspace of $H$.

We now construct an $\{r, s\}$-subgroup not contained in a conjugate of $H$. Take a Sylow $r$-subgroup from $F_q^\times$ as embedded in $GL(a, q)$, along with a non-trivial $s$-group of scalar (hence central) matrices. These commute, and thus form a group $L'$. Let

$$U = U'_1 \oplus U'_2 \oplus \cdots \oplus U'_m \oplus W'$$

be a decomposition of $n$-dimensional space with $\dim U'_i = a$ for each $i$. Since $\dim U'_i = a = r - 1 = \dim U_i - 1$, we have $\dim W' = c + m$. Let $L_i$ be the group acting as $L'$ on $U_i$ and trivially elsewhere. Then let

$$L = L_1 \times L_2 \times \cdots \times L_m$$
be the direct product. Since \(|L|_r = r^{[n/a]}\), \(L\) contains a full Sylow \(r\)-subgroup of \(GL(n, q)\).

Suppose that \(L\) is conjugate to a subgroup \(L^x\) of \(H\). By a further conjugation if necessary, we may assume that \(R \subseteq L^x\). We will derive a contradiction by comparing the number of invariant vectors of \(L^x\) with the number of those of the subgroups of \(H\). An \(r\)-cycle in \(R_i\) leaves invariant only the 1-dimensional space spanned by

\[ v_i = \sum_{j=1}^{r} e_{(i-1)r+j} \in U_i \quad \text{for} \quad i = 1, 2, \ldots, m. \]

Since \(R\) acts trivially on \(W\), \(R\) also leaves invariant

\[ v_{m+k} = e_{mr+k} \in W \quad \text{for} \quad k = 1, 2, \ldots, c. \]

Thus the \(R\)-invariant vectors span a space

\[ U_0 = \langle v_1, v_2, \ldots, v_{m+c} \rangle \]

of dimension \(m + c\).

Since \(L\) acts trivially on \(W'\), \(L\) leaves \(m + c\) linearly independent vectors invariant. Conjugation preserves the number of invariant vectors, so \(L^x\) must also act trivially on a space of dimension at least \(m + c\). But this space must be \(U_0\) because \(R \subseteq L^x\) leaves only the vectors in \(U_0\) invariant. By assumption, \(L^x \subset H\). Thus to complete the proof it suffices to show that no \(\{r, s\}\)-subgroup of \(H\) properly containing \(R\) leaves all the vectors in \(U_0\) invariant. We have already seen that the Sylow \(r\)-subgroup \(R\) of \(H\) acts trivially on \(U_0\). Recall that \(S\) consists of diagonal matrices. Let

\[ y = \text{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n) \]

be an element of \(S\). Assume that the subgroup \(\langle R, y \rangle\) of \(H\) is contained in \(L^x\). Then \(y\) sends the vector \(\sum \alpha_i e_i\) to \(\sum \sigma_i \alpha_i e_i\). Therefore \(yw_i = v_i\), for \(i = 1\) to \(n\), only if \(y = 1\). It follows that \(L^x = R\) is an \(r\)-group, which is not the case. This contradiction shows that \(L\) is not conjugate to a subgroup of \(H\), and \(D_{r,s}\) fails.

However, in the remaining cases, we will have a theorem to show that \(D_{r,s}\) holds. We will need the following lemma in order to apply induction.

**Lemma 3.2.** Assume the conditions for \(E_{r,s}\) in \(GL(n, q)\) hold in Case III of Theorem 2.1. Let \(X\) be a maximal \(\{r, s\}\)-subgroup of \(GL(n, q)\) acting naturally on an \(n\)-dimensional space \(U\). If \(X\) acts irreducibly on a subspace \(W\) of \(U\), then \(X\) acts primitively on \(W\). If in addition \(X\) acts non-trivially on \(W\), then \(\dim W\) is divisible by \(b\).
Proof. If \( X \) is not primitive on \( W \), then let \( W = W_1 \oplus W_2 \oplus \cdots \oplus W_k \) be a system of imprimitivity. Since \( X \) is irreducible, \( X \) does not consist entirely of permutation matrices. Thus \( X \) acts non-trivially on \( W_1 \) and \( \dim W_1 \geq a \). But \( X \) is an \( \{ r, s \} \)-group, and \( k \) is a divisor of \( |X| \). Thus \( k \geq r \). Then \( n = k \dim W_1 \geq ar \), a contradiction. This proves the first statement.

Assume that \( X \) acts non-trivially on \( W \). By Theorem 1.6, \( X \) is contained in a group \( G \) of type \( \mathcal{S} \) with field degree \( d \). Since \( X \) is an \( \{ r, s \} \)-group acting non-trivially on \( W \), either \( a \) or \( b \) divides \( \dim W \). If \( b \mid \dim W \), we are done, so assume that \( a \mid \dim W \). We will show that \( X \) acts on \( W \) as an \( r \)-group. We have

\[
\frac{\dim W}{d} \leq \frac{n}{d} < r < s.
\]

Should \( s \mid d \), then \( d \geq as \) since either \( a \) or \( b \) divides \( d \) and since \( s > b > a \). This contradicts \( d \leq n < ar < as \).

We now show that \([ G : V ]\) is prime to \( s \). If not, then by Lemma 1.7 with \( n \) replaced by \( \dim W \), we have \( s = (n/d) + 1 \). But by Theorem 2.1, \( n/d \leq n/a < r \). This contradicts the fact that \( r \) and \( s \) are two distinct odd primes. Therefore \([ G : F ]\) is prime to \( s \). Also, \( |F|_s = |q^d - 1|_s = 1 \) since \( b \nmid d \). Hence \( |X|_s = |G|_s = 1 \), as claimed.

We now show that \( b \) divides the dimension of \( W \). Decompose \( U \) as a direct sum

\[
U = W_1 \oplus W_2 \oplus \cdots \oplus W_k
\]

of \( X \)-irreducible subspaces \( W_i \). Suppose that at least one \( W_i \) has dimension divisible by \( a \). Let \( n_i = \dim W_i \) and \( c_0, c_1, \) and \( c_2 \) be defined by

\[
c_0 = \sum_{\dim W_i = 1} \dim W_i;
\]

\[
c_1 = \frac{1}{a} \sum_{a \mid \dim W_i} \dim W_i;
\]

\[
c_2 = \frac{1}{b} \sum_{b \mid \dim W_i} \dim W_i.
\]

Then (using \( b = r \)) \( n = c_0 + c_1 a + c_2 r \). We also have

\[
\left[ \begin{array}{c} n \\ a \end{array} \right] = \left[ \begin{array}{c} c_1 a + c_2 r + c_0 \\ a \end{array} \right] \geq c_1 + c_2.
\]
Assume first that \( c_0 < c_1 \). Then

\[
\left[ \frac{n}{r} \right] = \left[ \frac{c_1 a + c_2 r + c_0}{r} \right] < \left[ \frac{c_1 r + c_2 r}{r} \right] = c_1 + c_2,
\]

where the strict inequality holds because \( c_1 a + c_2 r + c_0 < c_1 r + c_2 r \). This is a contradiction to \( \left[ \frac{n}{a} \right] = \left[ \frac{n}{r} \right] \). Then \( c_0 \geq c_1 > 0 \).

Let \( W_i \) be an \( X \)-irreducible subspace of dimension \( ma \). Then \( m \leq c_1 \). Since \( c_0 \geq c_1 \geq m \), there is a space \( W_0 \) of dimension \( m \) on which \( X \) acts trivially. Let \( \bar{W} = W_0 \oplus W_i \). Then \( \dim \bar{W} = m + ma = mr \). Let \( \bar{X} = X/C_X(W) \) be the group that \( X \) induces on \( W \). Since \( W \) is a direct summand of \( U \), \( \bar{X} \) is a maximal \( \{r, s\} \)-subgroup of \( GL(\bar{W}) \).

Now \( \dim \bar{W} = mr \leq n < ar \) and \( \left[ \frac{mr}{r} \right] = \left[ \frac{mr}{a} \right] = m \). Therefore \( GL(\bar{W}) \) satisfies \( E_{r,s} \). Let \( H \) be a Hall subgroup of \( GL(\bar{W}) \). Then \( \bar{X} \) embeds in a conjugate of a Sylow \( r \)-subgroup of \( H \). By replacing \( H \) by a conjugate, we may assume that \( \bar{X} \subset H \). But \( \bar{X} \) is a maximal \( \{r, s\} \)-group, so \( \bar{X} = H \). This contradicts the fact that \( \bar{X} \) is an \( r \)-group. Thus \( c_1 = 0 \), and any irreducible \( X \)-subspace \( W \) has dimension divisible by \( b \) unless \( X \) acts trivially on \( W \) and \( \dim W = 1 \).

**Theorem 3.3.** Assume that the conditions for \( E_{r,s} \), given in Theorem 2.1, hold either in Case I or in Case III. Then \( D_{r,s} \) holds.

**Proof:** Let \( U \) be the space on which \( GL(n, q) \) acts, and let \( L \) be a maximal \( \{r, s\} \)-subgroup of \( GL(n, q) \). It suffices to show that \( L \) is a Hall subgroup. We will prove that \( L \) has a normal subgroup \( S \) with \( |S| = |GL(n, q)|/s \). The proof proceeds by induction on \( n \).

Assume the following inductive hypothesis: If \( GL(n', q) \) satisfies \( E_{r,s} \) with \( n' < n \), then a maximal \( \{r, s\} \)-group \( L' \) is a Hall subgroup of \( GL(n', q) \) and the Sylow \( s \)-subgroup of \( L' \) is normal in \( L' \). The proof divides according to the following three cases.

**Case 1:** \( L \) is reducible. In this case, \( U = W_1 \oplus \cdots \oplus W_k \) with each \( W_i \) \( L \)-irreducible. Let \( n_i = \dim W_i \). Define \( L_i \) to be the group induced by \( L \) on \( W_i \). That is, \( L_i = L/C_L(W_i) \). Then \( L \) is isomorphic to a subgroup of \( L_1 \times \cdots \times L_k \) with \( L_i \subset GL(W_i) \). By the maximality of \( L \), \( L = L_1 \times L_2 \times \cdots \times L_k \) and \( L_i \) is a maximal \( \{r, s\} \)-subgroup of \( GL(W_i) \). In order to apply the induction, we must show that \( GL(n_i, q) \) satisfies \( E_{r,s} \).

We must show that if \( E_{r,s} \) holds in \( GL(n, q) \), then \( E_{r,s} \) holds in \( GL(n_i, q) \). In Case I, if \( n < as \) then \( n_i < n < as \), as required. In Case III, we similarly get \( n_i < n < ar \). But we must also show that \( \left[ \frac{n_i}{a} \right] = \left[ \frac{n_i}{r} \right] \) for each \( i \).

By Lemma 3.2, \( r \mid \dim W_i \). If \( \dim W_i = 1 \), then \( E_{r,s} \) holds.
trivially. But if \( r \mid \dim W_i \), then \( \dim W_i/r = \dim W_i/a \), and \( GL(W_i) \) satisfies \( E_{r,s} \) in this case also.

By induction, each \( L_i \) is a Hall subgroup of \( GL(W_i) \). Let \( S_i \) be the normal Sylow \( s \)-subgroup \( S_i \) of \( L_i \) with

\[
|S_i| = |GL(n_i, q)|_s = q^b - 1 \left[ \frac{n_i}{b} \right], \quad \text{for } i = 1, 2, \ldots, k.
\]

Since \( n < bs \) in either Case I or Case III, \( \left[ \frac{n_i}{b} \right]_s = 1 \) for all \( i \). Let \( S = S_1 \times S_2 \times \cdots \times S_k \). We will show that \( S \) is the required normal Sylow \( s \)-subgroup of \( L \). Clearly, \( S \) is a normal subgroup of \( L \). Assume then that \( |S| < \left| GL(n, q) \right|_s \). By induction, we need only consider the case \( k = 2 \). We have

\[
|S| = |S_1| |S_2| = q^b - 1 \left[ \frac{n_1}{b} \right] + \left[ \frac{n_2}{b} \right] < q^b - 1 \left[ \frac{n}{b} \right].
\]

This implies that \( \left[ \frac{n_1}{b} \right] + \left[ \frac{n_2}{b} \right] < \left[ \frac{n}{b} \right] \). Since \( n = n_1 + n_2 \), we have \( \left\{ \frac{n_1}{b} \right\} + \left\{ \frac{n_2}{b} \right\} \geq 1 \), where \( \left\{ \frac{n_i}{b} \right\} \) indicates the fractional part of \( \frac{n_i}{b} \).

We know from the structure of the Sylow subgroups that \( S_i \) has \( \left[ \frac{n_i}{b} \right] \) invariant \( b \)-dimensional spaces. Therefore, \( S_i \) acts trivially on a space of dimension \( n_i - b\left[ \frac{n_i}{b} \right] = b\left\{ \frac{n_i}{b} \right\} \). Let \( W_0 \) be the space of all vectors on which \( S \) acts trivially. Then \( \dim W_0 = b\left\{ \frac{n_1}{b} \right\} + b\left\{ \frac{n_2}{b} \right\} \geq b \). Since \( S \leq L \), \( W_0 \) is \( L \)-invariant.

Let \( L_0 \) be the restriction \( L|_{W_0} \) of \( L \) to \( W_0 \). Since \( W_0 \) is \( L \)-invariant and \( L \) is maximal, \( L_0 \) is a direct factor of \( L \). Moreover, \( L_0 \) is a maximal \( \{r, s\} \)-subgroup of \( GL(W_0) \) because of the maximality of \( L \). Since \( \dim W_0 < n \), \( L_0 \) is a Hall \( \{r, s\} \)-subgroup of \( GL(W_0) \) by induction. Also, \( |L_0| \neq 1 \) since \( \dim W_0 \geq b \). But by the definition of \( W_0 \), \( L_0 \) is an \( r \)-group. This contradiction shows that \( |S| = \left| GL(n, q) \right|_s \). Thus \( S = S_1 \times S_2 \) is a full Sylow \( s \)-subgroup of \( GL(n, q) \), normal in \( L \), as required.

**Case 2:** \( L \) is irreducible but imprimitive. In Case III, this case is impossible by Lemma 3.2. So we must be in Case I. Let \( U \) be the space of dimension \( n \) on which \( L \) acts irreducibly. Also, let \( U = W_1 \oplus W_2 \oplus \cdots \oplus W_k \) be a decomposition of \( U \) into systems of imprimitivity. All \( W_i \) have the same dimension, say \( n' \). By Lemma 5 in [7], \( L = P(L_1 \times L_2 \times \cdots \times L_k) \), where \( P \) is a permutation group on \( \{1, 2, \ldots, k\} \) and \( L_i \) is a maximal \( \{r, s\} \)-subgroup of \( GL(W_i) \). By induction, \( L_i \) is a Hall subgroup of \( GL(W_i) \). Let \( S_i \) be the normal Sylow \( s \)-subgroup of \( L_i \), and let \( S = S_1 \times S_2 \times \cdots \times S_k \). We claim that \( S \) is a normal Sylow \( s \)-subgroup of \( L \). Clearly, \( S \) is normal
in $L$. To show that $S$ is a Sylow $s$-subgroup, we compute its order. We have

$$|S| = |S_1| |S_2| \cdots |S_k| = |S_1|^k = (|q^a - 1|_{s^{n'/a}})[n'/a]|_s)^k,$$

the last equality by Lemma 1.2. Since $n' \leq n < as$, we have $[n'/a]|_s = 1$. Then the equation simplifies to

$$|S| = |q^a - 1|_{s^{n'/a}}.$$

By Definition 1.5 and Theorem 1.6, one of $a$ or $b$ divides $d$. But we are in Case I, where $a = b$, so $a|d$. Furthermore, $d|n'$, so we may conclude that $a|n'$. So $[n'/a] = n'/a$ and

$$|S| = |q^a - 1|_{s^{kn'/a}} = |q^a - 1|_{s^{n/a}}.$$

Thus $S$ is a Sylow $s$-subgroup of $GL(n, q)$, again using Lemma 1.2 and the fact that $n < as$. This completes the proof of the inductive hypothesis in this case.

Case 3: $L$ is primitive. By Theorem 1.6, $L$ embeds in a group of type $S$ with field degree $d$ and normal series $F \triangleleft A \triangleleft V \triangleleft G$ and satisfying the conditions of Definition 1.5.

We now use Lemma 1.7 to show that $[G : F]$ is prime to $s$. The hypotheses we need to check are that $n/d < s$ and that $d$ is prime to $s$. Either $a|d$ or $b|d$. In Case I, $n < as = bs$. In Case III, $n < ar < as$ and $n < ar = ab < rh < hs$. If $a|d$, then $n/d \leq n/a < s$. If, however, $b|d$, then $n/d \leq n/b$, which is also less than $s$.

We now show that $s \nmid d$. Since $d$ is a multiple of either $a$ or $b$, we may let $d - ca$ or $d = cb$. Assume, for a contradiction, that $s|d$. Since $(s, a) = 1 = (s, b)$, $d \geq as$ or $d \geq bs$. Then $d > n$, a contradiction since $d|n$. Therefore, $d$ is prime to $s$ as required.

Assume (for a contradiction) that $[G : F]$ is divisible by $s$. Then by Lemma 1.7, $s = 2^j + 1$ is a Fermat prime and $n/d = 2^j$. Since $r$ and $s$ are odd, Definition 1.5 implies that $n = d$, a contradiction, thus $[G : A]$ is prime to $s$.

First assume that $a = b$ and $ar|d$. Let $d = er^c$ with $r \nmid e$. Note that $a|e$ since $a < r$ and $a|d$, and recall that $s \nmid d$. Let $S$ be the Sylow $s$-subgroup of $F_\infty^\times$. Since $|(q^d - 1)/(q^a - 1)|_s = 1$, $S \subset F_\infty^\times$. Thus $S$ is in the center of $GL(n/a, q^a)$. We now show that $S$ is also in the center of $L$. Since $S \subset F$, and since $V$ is the centralizer of $F$ in $G$, $S$ is centralized by $V$. Now $G/V$ is isomorphic to a subgroup of Gal($F_\infty^\times/F_\infty^\prime$). An automorphism $\phi$ of
order \( r^c \) in this Galois group is given by \( \phi(x) = x^{4'} \). This leaves invariant a field of \( q^e \) elements. In particular, \( \phi \) leaves invariant the subfield \( F_{q^e} \) of \( F_{q^f} \). Hence \( \phi \) leaves \( S \) invariant since \( S \subset F_{q^e} \). Thus \( G/V \) and \( V \) both centralize \( S \), so \( G \) (and hence \( L \)) centralizes \( S \). Now assume that \( r \nmid d \) in Case I. We will again prove that \( L \) centralizes \( S \). In this case, \( d \) is prime to \( r \) and \( s \), so \( L \subset V \). But \( V \) is the centralizer of \( F \) and \( S \subset F \). Thus \( S \) is in the center of \( L \) in both cases.

Let \( R \) be a Sylow \( r \)-subgroup of \( L \). Consider the natural embedding of \( GL(n/a, q^n) \subset GL(n, q) \). Since \( |GL(n/a, q^n)|_{r,s} = |GL(n, q)|_{r,s} \), there is a Hall subgroup \( H \) of \( GL(n, q) \) contained in \( GL(n/a, q^n) \). Then \( H \) and \( R \) are both contained in \( C_\sigma(S) \). By Sylow's Theorem, \( R^x \subset H \) for some \( x \in C_\sigma(S) \). But then \( L^x \subset H \) since \( S^x = S \). This proves the theorem in Case I.

Now assume we are in Case III. If \( b \nmid d \), then \( |L|_s = 1 \) and \( L \) is an \( r \)-group. But then \( L \) embeds in a Hall subgroup since \( E_{r,s} \) holds. Thus \( |F|_s > 1 \) and \( b|d \). Since \( n < ar \) and since \( b \leq d \), we have \( n/d \leq n/b = n/r < a < r \). By Lemma 1.7 with \( s \) replaced by \( r \), \( [V : F] \) is prime to \( r \). But \( d \) is divisible by \( b \) and not by \( a \), so \( |F| \) is also prime to \( r \). We may conclude that \( |V|_r = 1 \). Then the Sylow \( r \)-subgroup of \( L \) is isomorphic to a subgroup of \( G/V \) which is a cyclic group of order \( d \). In Case III, \( n < ar < r^2 \), so \( r \| d \).

Then \( |L| = rs^r \) where \( s^r = |q^b - 1|_s \).

Over \( F_q \), there are \( (s^r - 1)/r \) distinct irreducible representations of \( L \) of degree \( r \) nontrivial on the Sylow \( s \)-subgroup. By Theorem 47.11 and Remark (1), page 600, in [2], there is no other irreducible representation which is non-trivial on the Sylow \( s \)-subgroup. Since \( L \) is irreducible, we have \( n = r = b = d \).

Then

\[
|GL(n, q)|_{r,s} = |q^r - 1|_s r
\]
in Case III, so \( L \) is a Hall subgroup of \( GL(n, q) \). This completes the proof of the inductive hypothesis.

Let \( H \) be a Hall subgroup of \( GL(n, q) \). We may assume that \( S \subset H \). Let \( R_0 \) be the Sylow \( r \)-subgroup of \( L \) and let \( R \) be the Sylow \( r \)-subgroup of \( H \). By Sylow's Theorem applied to \( N(H) \), \( R_0 \) is conjugate, within \( N(H) \), to a subgroup of \( R \). This conjugation leaves \( S \) invariant, so it carries \( L \) into \( H \).

REFERENCES

