Notre Dame Journal of Formal Logic
Volume 28, Number 2, April 1987

Maximal p-Subgroups and the Axiom of Choice

PAUL E. HOWARD and MARY YORKE*

According to Sylow's well-known theorem, if p is a prime any finite group G has a Sylow p-subgroup, that is, a subgroup of order p^k where p^k is the highest power of p which divides the order of G.

The notion of Sylow p-subgroups has been generalized to infinite groups (see, for example, [5], p. 58; [2], Sections 54 and 85; and [6], Chapter 6) by the following:

Definition *A* Sylow p-subgroup of G is a maximal p-subgroup of G.

With this definition, the generalization of the Sylow theorem (ST) to infinite groups, i.e.,

ST *If p is a prime, every group has a Sylow p-subgroup*

is an easy consequence of Zorn's lemma.

We show in Section 2 that ST is actually equivalent to Zorn's lemma by showing ST implies the axiom of choice.

Section 3 contains a weakened version of ST, and its relationship to the axiom of choice for sets of finite sets is studied.

1 Definitions and preliminary results We will follow the usual convention of denoting a group $(G, \circ)$ by G when the choice of notation for the operation on the group does not concern us. If y is a set, we will denote by S_y the symmetric group on y. If $\sigma, \tau \in S_y$, $\sigma \circ \tau$ is the permutation defined by $(\sigma \circ \tau)(t) = \sigma(\tau(t))$.

If $t_1, t_2, \ldots, t_n \in y$, $(t_1; \ldots; t_n)$ denotes the cycle σ defined by

$$\sigma(t_i) = \begin{cases} t_{i+1} & \text{if } 1 \leq i < n \\ t_1 & \text{if } i = n, \end{cases}$$

and $\sigma(t) = t$ otherwise.

*The results of this paper were presented at the 817th meeting of the American Mathematical Society and appeared in the Abstracts of the American Mathematical Society number 84T-03-404.

Received April 22, 1985; revised September 4, 1985

(The notation $(t_1, \ldots, t_n)$ is reserved for the sequence of length n.) If $\{G_y: y \in Y\}$ is a set of groups, $\pi_{y\in Y} G_y$ will denote the weak direct product of the groups G_y, $y \in Y$. For each $y_0 \in Y$, we denote by P_{y_0} the projection map of $\pi_{y\in Y} G_y$ onto G_{y_0}.

If G is a group and p is a prime, a p-subgroup of G is a subgroup of G each of whose elements has order a power of p.

The following two theorems will be used in Sections 2 and 3:

Theorem 1.1 *If H is a maximal p-subgroup of $\pi_{y\in Y} G_y$, then $P_y(H)$ is a maximal p-subgroup of G_y for each $y \in Y$.*

Theorem 1.2 *If H_y is a maximal p-subgroup of G_y for each $y \in Y$, then $\pi_{y\in Y} H_y$ is a maximal p-subgroup of $\pi_{y\in Y} G_y$.*

We omit the proofs, which are straightforward and do not use the axiom of choice.

We will use the following abbreviations:

$S(p)$: Every group has a maximal p-subgroup.
S: $(\forall p)$ (p is a prime $\rightarrow S(p)$).
$SPF(p)$: If $\{G_y: y \in Y\}$ is a set of finite groups, then $\pi_{y\in Y} G_y$ has a maximal p-subgroup.
SPF: $(\forall p)$ (p a prime $\rightarrow SPF(p)$).
$SPS(p)$: If Y is a set of nonempty, finite sets, then $\pi_{y\in Y} S_y$ has a maximal p-subgroup, where S_y is the symmetric group on y.
SPS: $(\forall p)$ (p a prime $\rightarrow SPS(p)$).

We will also use the notation:

AC: The axiom of choice.
AC_{fin}: If Y is a set of nonempty, finite sets, then Y has a choice function.
AC_n: If Y is a set of n-element sets, then Y has a choice function.

And finally, if K is an infinite subset of the natural numbers,

AC_K: If Y is a set such that $(\forall y \in Y)(|y| \in K)$ then Y has a choice function.

2 *S and AC*

In this section we will denote the finite sequence $\vec{t} = (t_1, \ldots, t_n)$ by $t_1 \ldots t_n$ and $L(\vec{t})$ will denote the length of $\vec{t}$. Further t^q will denote the finite sequence $(t, t, \ldots, t)$ of length q.

Our goal is to prove

Theorem 2.1 *If p is any prime, then $S(p)$ implies AC.*

Proof: Let Y be a set of nonempty sets. For each $y \in Y$, let $(G_y, {}^*)$ be the group defined as follows: G_y is the set of all finite sequences of elements of y such that no element of y occurs p consecutive times, that is, $G_y = \{t_1 \ldots t_n: t_j \in y$ for $1 \leq j \leq n$ and $(\forall k \leq n - p + 1)$ $(t_k \neq t_{k+1}$ or $t_{k+1} \neq t_{k+2}$ or $\ldots$ or $t_{k+p-2} \neq t_{k+p-1})\}$. * is concatenation of sequences followed by deletions of subsequences of p consecutive, identical elements of y; that is, if $\vec{t} = t_1 \ldots t_n$ and $\vec{s} = s_1 \ldots s_k$ then $\vec{t}^*\vec{s} = t_1 \ldots t_j s_m \ldots s_k$ where

(1) for some natural numbers i and $d_1, d_2, \ldots, d_i$

$$t_{j+1} \ldots t_n = r_1^{d_1} \ldots r_i^{d_i} \text{ and}$$
$$s_1 \ldots s_{m-1} = r_i^{p-d_i} r_{i-1}^{p-d_{i-1}} \ldots r_1^{p-d_1}$$

and

(2) $t_1 \ldots t_j s_m \ldots s_k \in G_y$ ($t_1 \ldots t_j$ or $s_m \ldots s_k$ may be the empty sequence).

We note

(3) $L(\vec{t}*\vec{s}) < L(\vec{t}) + L(\vec{s})$ implies $t_n = s_1$.

($(G_y, *)$ is isomorphic to the group with the generators $\{t: t \in y\}$ and relations $\{t^p = 1: t \in y\}$, but the description given above is most convenient for our purposes.)

We now apply $S(p)$ to obtain a maximal p-subgroup H of $\pi_{y \in Y} G_y$. By Theorem 1.1, $P_y(H)$ is a maximal p-subgroup of G_y, for each $y \in Y$. Clearly $P_y(H) \neq \{1_y\}$ (1_y is the identity of G_y), since the sequence t (of length 1) for each $t \in y$ has order p.

Lemma 2.2 *If $\vec{t} = t_1 \ldots t_n$ is in $P_y(H)$, $n > 0$, then $t_1 = t_n$.*

Proof: Since $P_y(H)$ is a p-subgroup of G_y, $\vec{t}^k = \underbrace{\vec{t}*\vec{t}*\vec{t} * \ldots * \vec{t}}_{k \text{ factors}} = 1_y$ for some finite k. If $t_1 \neq t_n$ then clearly the length of $\vec{t}^k$ will be $k(L(\vec{t})) > 0 = L(1_y)$ a contradiction.

Lemma 2.3 *If $\vec{t} = t_1 \ldots t_n$ and $\vec{s} = s_1 \ldots s_k$ are in $P_y(H)$ then $t_1 = s_1$.*

Proof: Since $P_y(H)$ is a subgroup of G_y, $\vec{t}, \vec{s} \in P_y(H)$ implies $\vec{t}*\vec{s} \in P_y(H)$. We consider two cases: *Case 1.* $L(\vec{t}*\vec{s}) = L(\vec{t}) + L(\vec{s})$. In this case, $\vec{t}*\vec{s} = t_1 \ldots t_n s_1 \ldots s_k$ and by Lemma 2.2, $t_1 = s_k = s_1$. *Case 2.* $L(\vec{t}*\vec{s}) < L(\vec{t}) + L(\vec{s})$.

By (3) $t_n = s_1$, then by Lemma 2.2, $t_1 = s_1$. This completes the proof of Lemma 2.3. We now define a choice function f for Y as follows:

For each $y \in Y$, $f(y) =$ the unique element t of y such that $t_1 \ldots t_n \in P_y(H) \Rightarrow t_1 = t$.

3 SPF, SPS and AC_{fin} Clearly *SPF* implies *SPS* and, for any prime p, *SPF*(p) implies *SPS*(p). The fact that *SPF*(p) and *SPS*(p) are equivalent will follow from the next two theorems.

Theorem 3.1 *If p is a prime and $K = \{r \in \omega: gcd(r, p) = 1\}$ then $SPS(p) \Rightarrow AC_K$.*

Proof: Our proof will use the following:

Lemma 3.2 *If p is a prime and H is a p-subgroup of S_n (the symmetric group on $\{1, 2, \ldots, n\}$) and if $\sigma = (s_1; \ldots; s_p)$ and $\tau = (t_1; \ldots; t_p)$ are p cycles in H, then either*

$$\{s_1, \ldots, s_p\} = \{t_1, \ldots, t_p\}$$

or

$$\{s_1, \ldots, s_p\} \cap \{t_1, \ldots, t_p\} = \varnothing.$$

Proof: Suppose the lemma is false and that $\sigma = (s_1; \ldots; s_p)$ and $\tau = (t_1; \ldots; t_p)$ are two p cycles such that $\sigma, \tau \in H$,

(4) $\{s_1, \ldots, s_p\} \cap \{t_1, \ldots, t_p\} \neq \varnothing$

and

(5) $\{s_1, \ldots, s_p\} \neq \{t_1, \ldots, t_p\}$.

By (4) we may assume $s_1 = t_1$ and by (5) we assume $t_2 \notin \{s_1, \ldots, s_p\}$ (replacing τ by a suitable power of τ if necessary). If $\{s_1, \ldots, s_p\} \cap \{t_1, \ldots, t_p\} = t_1$ then $\tau \circ \sigma = (t_1; s_2; \ldots; s_p) \circ (t_1; \ldots; t_p) = (t_1; t_2; \ldots; t_p; s_2; \ldots; s_p) \in H$, contradicting our assumption that H is a p-group.

We therefore assume $t_k \in \{s_1, \ldots, s_p\}$ for some k, $2 < k \leq p$; say $t_k = s_m$ and that $t_j \notin \{s_1, \ldots, s_p\}$ for $2 \leq j < k$. Then since $\sigma^{p-m}(s_m) = s_p$, $\sigma^{p-m} \circ \tau \circ \sigma = (s_m; s_p; \ldots)(s_1; t_2; \ldots t_{k-1}; s_m; t_{k+1}; \ldots t_p)(s_1; \ldots; s_p) = (s_p; t_2; t_3; \ldots; t_{k-1}) \circ$ (some other disjoint cycles) $\in H$. But the cycle $(s_p; t_2; t_3; \ldots; t_{k-1})$ has length greater than 1 and less than p, again contradicting our assumption that H is a p-group. This proves Lemma 3.2.

For each finite set y and p-subgroup H of S_y we define the relation $R(y, H)$ (also denoted by R_y if H is fixed) by $t_1 R_y t_2$ if and only if $\sigma(t_1) = t_2$ for some p-cycle, $\sigma \in H$.

As a consequence of Lemma 3.2 we have

Lemma 3.3 *If H is a p-subgroup of S_y then $R(y, H)$ is an equivalence relation on y.*

We also have

Lemma 3.4 *If H is a Sylow p-subgroup of S_y and $|y| = kp + r$ where k and r are natural numbers $0 \leq r < p$ then $R(y, H)$ has k equivalence classes of cardinality p and r equivalence classes of cardinality* 1.

Proof: It suffices to prove the lemma for $y = \{1, 2, \ldots, n\}$ where $n = k \cdot p + r$, $0 \leq r < p$. Let K be the subgroup of S_y generated by the cycles $\sigma_1 = (1; 2; \ldots; p)$, $\sigma_2 = (p+1; p+2; \ldots 2p), \ldots, \sigma_k = ((k-1)p+1; (k-1)p+2; \ldots; kp)$. Clearly K is a p-subgroup, therefore K is contained in a Sylow-p subgroup H_0 of S_y. By Lemma 3.2 the conclusion of Lemma 3.4 holds for H_0. Using the fact that all Sylow-p subgroups of S_y are conjugate in S_y ([2], p. 59), the conclusion of Lemma 3.4 for every Sylow p-subgroup of S_y follows.

To complete the proof of Theorem 3.1 let Y' be a set such that $(\forall y \in Y')(|y| \in K)$. If $y \in Y'$, then there is a least positive integer n_y such that $|y| \cdot n_y \equiv 1 \mod p$.

Let $Y = \{y \times n_y : y \in Y'$ and $n_y = \{0, 1, \ldots, n_y - 1\}$ is the least positive integer such that $|y| \cdot n_y \equiv 1 \mod p\}$.

We will use $SPS(p)$ to construct a choice function for Y which will give a choice function for Y' (see [4]). Let $G = \pi_{y \in Y} S_y$. By $SPS(p)$, G has a maximal p-subgroup H. By Theorem 1.1, $P_y(H)$ is a Sylow p-subgroup of S_y for each $y \in Y$. By Lemma 3.4, $R(y, P_y(H))$ has exactly one equivalence class of cardinality 1. Therefore if we define for each $y \in Y$

> $f(y)$ = the element of the unique equivalence class of $R(y, P_y(H))$ with cardinality 1

we get a choice function for Y.

This completes the proof of Theorem 3.1.

Theorem 3.5 *If p is a prime and $K = \{r \in \omega : r \equiv 1 \text{ mod } p\}$, then AC_K implies $SPF(p)$.*

Proof: Let $\{G_y : y \in Y\}$ be a set of finite groups. For each $y \in Y$, let $W(y)$ be the set of Sylow p-subgroups of G_y. By [5], p. 59, Theorem 4.9, $|W(y)| \equiv 1$ *mod p* and, therefore, by AC_K, $\{W(y): y \in Y\}$ has a choice function f. By Theorem 1.2, $\pi_{y \in Y} f(W(y))$ is a maximal p-subgroup of $\pi_{y \in Y} G_y$.

Corollary 3.6 *Let p be a prime and let $K_1 = \{r \in \omega: gcd(r, p) = 1\}$ and $K_2 = \{r \in \omega: r \equiv 1 \text{ mod } p\}$. Then the following are equivalent:*

(i) $SPS(p)$
(ii) AC_{K_1}
(iii) AC_{K_2}
(iv) $SPF(p)$.

Corollary 3.7 *If $p_1 \neq p_2$ are primes, then $SPS(p_1)$ and $SPS(p_2)$ imply AC_{fin}.*

(This follows from Theorem 3.1.)

We now strengthen Corollary 3.7 to

Theorem 3.8 *If p is a prime then AC_p and $SPS(p)$ imply AC_{fin}.*

Proof: Let Y be a set of nonempty finite sets. Define by induction

$$Y_0 = Y$$
$$Y_{n+1} = \{z: (\exists y \in Y_n)(z \subseteq y)\} \cup \{w: (\exists y \in Y_n) \ (w \text{ is a partition of } y)\}.$$

Let $Y' = \bigcup_{n \in \omega} Y_n$, then Y' has the properties

(6) If $y \in Y'$ and $z \subseteq y$, then $z \in Y'$

(7) *If* $y \in Y'$ and w is a partition of y, then $w \in Y'$.

We will use AC_p and $SPS(p)$ to construct a choice function for Y' and therefore, since $Y \subseteq Y'$, a choice function for Y.

First note that by Theorem 3.1, AC_p and $SPS(p)$ give us a choice function f_0 for $\{y \in Y': |y| \leq p\}$. Now a direct application of $SPS(p)$ gives us a maximal p-subgroup H of $\pi_{y \in Y'} S_y$. Define a choice function f on Y' by induction as follows:

If $y \in Y'$ and $|y| \leq p$, $f(y) = f_0(y)$. Suppose now that $y \in Y'$, $|y| = n > p$ and that $f(y')$ has been defined for every $y' \in Y$ such that $|y'| < n$. By Theorem 1.1, $P_y(H)$ is a maximal p-subgroup of S_y. Since $|y| > p$, Lemma 3.4 implies that $R(y, P_y(H))$ has more than 1 and fewer than n-equivalence classes. By the Induction assumption and (7), $f(w)$ is defined and $f(w) \subseteq y$ where $w =$

$\{c: c$ is an R_y equivalence class$\}$ and therefore by (6) $f(f(w))$ is defined and $f(f(w)) \in y$. We define $f(y) = f(f(w))$.

This completes the proof of Theorem 3.8.

Using Theorem 1.2 it is easy to see that $AC_{fin} \Rightarrow SPF$. We therefore have

Corollary 3.9 *If p_1 and p_2 are primes, and $p_1 \neq p_2$, then the following are equivalent*

(i) AC_{fin}
(ii) $SPS(p_1) \wedge SPS(p_2)$
(iii) AC_{p_1} and $SPS(p_1)$
(iv) SPF
(v) SPS.

That Theorem 3.1 and Corollary 3.6 are, in some sense, the best possible results, is shown by the following.

Theorem 3.10 *If p is a prime $SPS(p) \nRightarrow AC_p$.*

Proof: We show that no proof of AC_p from $SPS(p)$ is possible in ZFU (Zermelo-Frankel set theory weakened to permit the existence of urelements) by constructing a permutation model of ZFU in which $SPS(p)$ is true and AC_p is false. We refer the reader to [1] for elementary facts about permutation models.

Finally we will indicate how the independence result can be transferred to ZF.

Let M' be a model of $ZFU + AC$ and suppose the set of urelements $\mathsf{U} = \bigcup_{n\in\omega} A_n$ where $A_i \cap A_j = \varnothing$ if $i \neq j$ and $|A_i| = p$ for $i \in \omega$. Let ψ_i be a (fixed) permutation of A_i which is a p cycle. Let $G = \{\phi: \phi$ is a permutation of U and $(\forall i \in \omega)(\phi|A_i = \psi_i^n$ for some integer $n)$ and $(\exists k \in \omega)(\forall j > k)(\forall t \in A_j)(\phi(t) = t)\}$ ($\phi|A_i$ denotes the restriction of ϕ to A_i). Clearly $\phi \in G \Rightarrow \phi^p = 1$.

Note that $\phi \in G$ can be extended uniquely to all of M' by ϵ-induction. The extension is also denoted by ϕ. If $E \subseteq \mathsf{U}$, let $fix\ (E) = \{\phi \in G: (\forall t \in E)(\phi(t) = t)\}$ and let F be the filter of subgroups of G generated by $\{fix\ (E): E \subseteq \mathsf{U}$ and E is finite$\}$. If $x \in M'$ and there is some finite $E \subseteq \mathsf{U}$ such that $\phi \in fix(E) \Rightarrow \phi(x) = x$ we say E is a (finite) support of x.

Let M be the permutation model determined by F and G, that is, M consists of those elements $x \in M'$ such that x and each element of the transitive closure of x have finite support.

Claim 1 AC_p is false in M.

For $Y = \{A_n: n \in \omega\}$ is a set of p-element sets in M (with support $\varnothing$). Suppose f is a choice function for Y in M with finite support E. Since E is finite, there is some $A_n \in Y$ such that $A_n \cap E = \phi$ and therefore ϕ defined by

$$\phi(t) = \begin{cases} \psi_n(t) & t \in A_n \\ t & \text{otherwise} \end{cases}$$

is in $fix\ (E)$. ϕ fixes Y and A_n but $\phi(f(A_n)) \neq f(A_n)$ since $f(A_n) \in A_n$. Therefore E is not a support of f.

The proof of Theorem 3.10 is completed by showing

Claim 2 $SPS(p)$ is true in M.

Let Y be a collection of finite sets in M and let $W = \pi_{y \in Y} S_y$. We show W has a maximal p-subgroup in M. Suppose Y has finite support E. For each $y \in Y$ let $OB(y)$ be the *fix* (E) orbit of y, i.e., $OB(y) = \{\phi(y): \phi \in fix\ (E)\} \subseteq Y$.

Let F be a choice function for $\{OB(y): y \in Y\}$ (F is in M' but not necessarily in M). Let $X = \{F(OB(y)): y \in Y\}$ and for each $y \in X$, let $L(y)$ be a Sylow p-subgroup of S_y containing the p-subgroup $\{\phi | y: \phi \in fix\ (E)$ and $\phi(y) = y\}$.

Lemma 3.11 *If $y \in X$ and $\phi, \psi \in fix\ (E)$ and $\phi(y) = \psi(y)$, then $\phi(L(y)) = \psi(L(y))$.*

Proof: Assume the hypotheses, then $\psi^{-1}(\phi(y)) = y$ and $\psi^{-1} \circ \phi \in fix\ (E)$; hence $\psi^{-1} \circ \phi | y \in L(y)$; therefore $(\psi^{-1} \circ \phi)(L(y)) = ((\psi^{-1} \circ \phi | y) L(y) ((\psi^{-1} \circ \phi | y)^{-1})) = L(y)$. So $\phi(L(y)) = \psi(L(y))$, proving the lemma. (We have used the fact that if η and σ are permutations, then $\eta(\sigma) = \eta \circ \sigma \circ \eta^{-1}$.)

Hence $T = \{\phi((y, L(y))): y \in X$ and $\phi \in fix\ (E)\}$ is a function in M with domain Y and for each $y \in Y$, $T(y)$ is a Sylow p-subgroup of S_y. Therefore by Theorem 1.2, $\pi_{y \in Y} T(y)$ is maximal p-subgroup of $\pi_{y \in Y} S_y$ in M proving Claim 2.

To transfer the result to Zermelo-Frankel set theory we note that by Corollary 3.6, AC_K holds in M where $K = \{r \in \omega: gcd(r, p) = 1\}$. By an argument almost identical to the one in [1], p. 109, we can construct a model N of ZF from M in which AC_p fails and AC_K holds. Therefore by Corollary 3.6 $SPS(p)$ holds in N.

As a final remark, we note that several negative results can be obtained using the theorem of Levy [3]:

$$ZFU \nvdash (\forall n \in \omega)(AC_n) \rightarrow AC_{fin}.$$

Let p be a prime. By Corollary 3.9, AC_p and $SPS(p) \rightarrow AC_{fin}$. Therefore

$$ZFU \nvdash (\forall n \in \omega)(AC_n) \rightarrow SPS(p).$$

Using Corollary 3.6, we also obtain

$$ZFU \nvdash (\forall n \in \omega)(AC_n) \rightarrow AC_{K_1}$$

and

$$ZFU \nvdash (\forall n \in \omega)(AC_n) \rightarrow AC_{K_2}.$$

REFERENCES

[1] Jech, T., *The Axiom of Choice*, North-Holland Publishing Company, Amsterdam, 1973.

[2] Kurosh, A. G., *The Theory of Groups*, trans. K. A. Hirsch, Chelsea Publishing Company, New York, 1955.

[3] Levy, A., "Axioms of multiple choice," *Fundamenta Mathematica*, vol. 50 (1962), pp. 475–483.

[4] Mostowski, A., "Axiom of choice for finite sets," *Fundamenta Mathematica*, vol. 33 (1945), pp. 137–168.

[6] Rotman, J., *An Introduction to the Theory of Groups*, Allyn and Bacon Publishing Company, Newton, Massachusetts, 1984.

[6] Shenkman, E., *Group Theory*, Robert E. Krieger Publishing Company, New York, 1975.

[7] Scott, W. R., *Group Theory*, Prentice Hall, Englewood Cliffs, New Jersey, 1964.

Department of Mathematics
Eastern Michigan University
Ypsilanti, Michigan 48197