Transitive permutation groups of prime-squared degree

Dave Witte

Department of Mathematics
Oklahoma State University
Stillwater, OK 74078

dwitte@math.okstate.edu

Main author:

Edward Dobson

Department of Mathematics and Statistics
Mississippi State University
Mississippi State, MS 39762

dobson@math.msstate.edu

Thm (Burnside). *Let*

- *G be a transitive perm grp of degree p; and*
- *P be a Sylow p-subgroup of G.*

Then either

1) *$P \lhd G$; or*
2) *G is doubly transitive.*

This leads a complete classification of permutation groups of degree p.

1) $|G|_p = p \quad \Rightarrow P \sim$ regular rep of $\mathbb{Z}_p$,
so $G \hookrightarrow N_{S_p}(\mathbb{Z}_p) = \mathrm{Aff}(1,p) \cong \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$.

Choice of $G \quad \leftrightarrow \quad$ divisor d of $p-1$

$$|\,\mathrm{Aff}(1,p) : G| = d.$$

2) Classification of Finite Simple Groups,
$\Rightarrow$ all doubly transitive groups are known.

Want to do the same for groups of degree p^2.

Thm. *Let*

- $H \leq S_p$ *doubly transitive;*
- S *be a min'l normal subgroup of* H*; and*
- $N = N_{S_p}(S)$.

Then S *is simple,* $S \leq H \leq N$, N/S *is cyclic, and, after replacing* H *by a conjugate, either:*

- $S = \mathbb{Z}_p$, $N = A(1,p)$, *and* $N/S \cong \mathbb{Z}_{p-1}$*; or*
- $S = A_p$, $N = S_p$, *and* $N/S \cong \mathbb{Z}_2$*; or*
- $p = 11$ *and* $S = H = N = \mathrm{PSL}(2,11)$*; or*
- $p = 11$ *and* $S = H = N = M_{11}$*; or*
- $p = 23$ *and* $S = H = N = M_{23}$*; or*
- $p = \dfrac{q^d - 1}{q - 1}$ *for some* $q = r^m$ *and* d*, and* $S = \mathrm{PSL}(d,q)$, $N = \mathrm{P\Gamma L}(d,q)$, $N/S \cong \mathbb{Z}_m$.

Conj. $\exists\ \infty$ *primes of the form* $(q^d - 1)/(q - 1)$.
E.g. any Mersenne prime $p = 2^d - 1$.

Thm (Wielandt). *Let* $G \leq S_{p^2}$ *transitive. Then*

1) $P \triangleleft G$*; or*
2) G *is doubly transitive; or*
3) G *is imprimitive; or*
4) G *has an imprimitive subgroup of index* 2*, and* $P \cong \mathbb{Z}_p \times \mathbb{Z}_p$*, for any* $P \in \mathrm{Syl}_p(G)$.

Defn. Let G act transitively on Ω.

- $B \subset \Omega$ is a *block* if $1 < |B| < |\Omega|$ and
  $\forall g \in G,$ either $Bg = B$ or $Bg \cap B = \emptyset$.
  I.e., $\mathcal{B} = \{ Bg \mid g \in G \}$ partitions Ω.
- G is *imprimitive* if $\exists$ block B.

2) Use the classification of dbly transitive grps.

a) $\mathbb{Z}_p^2 < H \leq \mathrm{Aff}(2, p)$

b) A_{p^2}, S_{p^2}

c) $\mathrm{PSL}(d, q) \leq H \leq \mathrm{P\Gamma L}(d, q)$

a) C. Hering [Huppert III, Rmk. XII.7.5, p. 386]

Analogue of Burnside's Theorem.

Main Thm. *$G \leq S_{p^2}$ transitive, $P \in \mathrm{Syl}_p(G) \Rightarrow$*

1) *$P \lhd G$; or*
2) *G is doubly transitive; or*
3) *$\exp(P) = p$ and $|P| \in \{p^2, p^p\}$; or*
4) *$|P| = p^{p+1}$.*

Prop. *$G \leq S_{p^2}$ imprim, P elem abel of order p^2*
$\Rightarrow G$ is equivalent to a subgroup of $S_p \times S_p$.

Defn. Let $H, L \leq S_p$. Then

$$H \wr L = H \ltimes L^p \hookrightarrow S_{p^2},$$

where $(l_1, \ldots, l_p)^h = (l_{1^{h^{-1}}}, \ldots, l_{p^{h^{-1}}})$.

$H \wr L$ acts faithfully on $\mathbb{Z}_p \times \mathbb{Z}_p$ by

$$(i, j)^h = (i^h, j)$$
$$(i, j)^{(l_1, \ldots, l_p)} = (i, j^{l_i})$$

$\{i\} \times \mathbb{Z}_p$ is a block, so $H \wr L$ is imprimitive.

Note that $e \wr L$ fixes each block.

Exer. Any imprimitive subgroup of S_{p^2} is equivalent to a subgroup of $S_p \wr S_p$.

Exer. $\mathbb{Z}_p \wr \mathbb{Z}_p$ is a Sylow p-subgrp of $S_{\mathbb{Z}_p \times \mathbb{Z}_p} \cong S_{p^2}$.

For $0 \leq i \leq p$, $\exists!$ $K_i \leq e_p \wr \mathbb{Z}_p \cong (\mathbb{Z}_p)^p$, s.t.

$$K_i \lhd \mathbb{Z}_p \wr \mathbb{Z}_p \text{ and } |K_i| = p^i.$$

E.g., $K_p = e_p \wr \mathbb{Z}_p$ and $K_{i-1} = [\mathbb{Z}_p \wr \mathbb{Z}_p, K_i]$.

Exer. If $P \leq \mathbb{Z}_p \wr \mathbb{Z}_p$, $P \not\leq K_p$, and $|P| = p^i$, then $P \cap K_p = K_{i-1}$.

Fact. $\mathbb{Z}_p \ltimes K_{p-1}$ is the unique transitive subgroup of $\mathbb{Z}_p \wr \mathbb{Z}_p$ with exponent p and order p^p.

$$K_{p-1} = \{(z_1, \ldots, z_p) \in (\mathbb{Z}_p)^p \mid \textstyle\sum_{i=1}^{p} z_i = 0\}.$$

Fact. For $0 \le i < p$, $N_{e \wr S_p}(K_i) = \mathbb{Z}_p^* \cdot K_p$.

Prop. *$G \le S_{p^2}$ imprim, $P = \mathbb{Z}_p \ltimes K_{p-1} \Rightarrow$ $\exists\ H \le S_p \times \mathbb{Z}_p^*$, s.t. G is equiv to $H \cdot K_{p-1}$.*

Eg. Let $H, L \le S_p$ transitive.

$G = H \wr L \le S_{p^2}$ is imprim, and $|G|_p = p^{p+1}$.

Prop. *$G \le S_{p^2}$ imprim, $|G|_p = p^{p+1}$. $\exists$*

1) *$H, L \le S_p$ transitive, such that L is simple;*
2) *$K/L^p \le \big(N_{S_p}(L)/L\big)^p$ H-invariant;*
3) *$\phi\colon H \to N_{S_p}(L)^p/K$ crossed homomorphism;*

such that G is equivalent to

$$\{\, (h, v) \in H \ltimes N_{S_p}(L)^p \mid \phi(h) = vK \,\}$$
$$\subset S_p \wr S_p.$$

Remaining problems.

For $\mathrm{PSL}(d,q) \le H \le \mathrm{P\Gamma L}(d,q)$:

1) Find H-invariant subgroups K of $(\mathbb{Z}_{r^k})^p$ (where $q = r^m$). ($k = 1$ done [Bardoe-Sin])
2) For each subgrp K,

   calculate $H^1\big(H, (\mathbb{Z}_{r^k})^p/K\big)$ and
   find an explicit rep of each coho class.

For $H = \mathrm{PSL}(2,11)$, M_{11}, M_{23}: Problem 2.

Main Thm. *Let* $G \leq S_{p^2}$*,* $P \in \mathrm{Syl}_p(G)$*. Then either* $P \lhd G$*, or* G *is doubly transitive, or* $|P| = p^{p+1}$*, or* $\exp(P) = p$ *and* $|P| \in \{p^2, p^p\}$*.*

Proof. Assume G is not dbly trans, $|P| \neq p^{p+1}$, and either $\exp(P) = p^2$ or $|P| \notin \{p^2, p^p\}$.

$P \not\cong \mathbb{Z}_p \times \mathbb{Z}_p$, so Wielandt's Thm $\Rightarrow$ G imprim.

Let $\mathcal{B}$ be a block system for G.

Defn. $\mathrm{Fix}_G(\mathcal{B}) = \{\, g \in G \mid \forall B \in \mathcal{B},\ Bg = B \,\}$.

Strategy: show $\mathrm{Fix}_G(\mathcal{B})$ and $G/\mathcal{B}$ are solvable.

Lem. G *solvable, imprimitive,* $|P| \neq p^{p+1}$
$\Rightarrow$ $P \lhd G$*.*

Lem. *G solvable, imprimitive, $|P| \neq p^{p+1}$*
$\Rightarrow P \triangleleft G$.

Proof. We always assume $P \leq \mathbb{Z}_p \wr \mathbb{Z}_p$.

We have $\mathrm{Fix}_P(\mathcal{B}) = K_p \cap P = K_i$ for some i.

$\mathrm{Fix}_G(\mathcal{B})$ solvable $\Rightarrow G \leq N_{S_p \wr S_p}(K_i)$.

Because $N_{S_p \wr S_p}(K_i)$ normalizes $\displaystyle\prod_{B \in \mathcal{B}} K_i|_B = K_p$,
then $G \leq N_{S_p \wr S_p}(K_p) = S_p \wr \mathrm{Aff}(1,p)$.

$G/\mathcal{B}$ solvable $\Rightarrow G \leq \mathrm{Aff}(1,p) \wr \mathrm{Aff}(1,p)$.

Because $p^1 < |P| < p^{p+1}$, we have $0 < i < p$,
so $N_{e \wr S_p}(K_i) = \mathbb{Z}_p^* \cdot K_p$.

Therefore $G \leq \big(\mathrm{Aff}(1,p) \times \mathbb{Z}_p^*\big) \cdot K_p$.

This has a unique Sylow p-subgroup.

Lem. *If* $|P| \neq p^{p+1}$ *and* $P \ncong \mathbb{Z}_p \times \mathbb{Z}_p$, *then* $\mathrm{Fix}_G(\mathcal{B})$ *is solvable.*

Proof. Let $N \leq \mathrm{Fix}_G(\mathcal{B})$ minimal normal in G. Suppose N is not a p-group, so $N = L_1 \times \cdots \times L_m$ is a direct product of nonabelian simple groups.

Defn. $\mathrm{supp}(L_i) = \{\, B \in \mathcal{B} \mid L_i|_B \neq e \,\}$.

$[L_i, L_j] = e \qquad \Rightarrow \mathrm{supp}(L_i) \cap \mathrm{supp}(L_j) = \emptyset.$

G-action on $\mathcal{B}$ is primitive

$\Rightarrow |\,\mathrm{supp}(L_i)| \in \{1, p\};$

$\Rightarrow m \in \{1, p\}.$

$m = p \Rightarrow (\mathbb{Z}_p)^p \hookrightarrow N \cap P$, so $|G|_p = p^{p+1}$. $\rightarrow\leftarrow$

$m = 1 \Rightarrow \mathrm{Fix}_G(\mathcal{B}) \subset N_{e \wr S_p}(L_1) \cong N_{S_B}(L_1|_B)$

(because $C_{S_{B'}}(L_1|_{B'}) = e$)

so $|\,\mathrm{Fix}_G(\mathcal{B})|_p = p$. Therefore $|P| = p^2$.

We now know $P \cong \mathbb{Z}_{p^2}$ (and $m = 1$).

Suppose P is cyclic ($\cong \mathbb{Z}_{p^2}$), and $m = 1$.

Let g be any p'-element of $N_{L_1}(P^p)$.

Because $P^p = K_1$, we know that $g \in \mathbb{Z}_p^* K_p$,
so g normalizes $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Therefore, $[P, g]$ is a p-subgroup of $\mathrm{Fix}_G(\mathcal{B})$.

Each of P and g normalizes P^p,
and P^p is a Sylow p-subgroup of $\mathrm{Fix}_G(\mathcal{B})$,
so $[P, g] \subset P^p$.

Therefore g normalizes P, and centralizes P/P^p.
Because g is a p'-element, then g centralizes P.

Thus, P^p is in the center of its normalizer in L_1,
so L_1 has a normal p-complement.

Because L_1 is simple, this is nonsense. $\rightarrow\leftarrow$

Lem. *Assume*

- $\mathrm{Fix}_G(\mathcal{B})$ *is solvable; and*
- $G/\mathcal{B}$ *is not solvable.*

Then $|P| \in \{p^2, p^p, p^{p+1}\}$.

Proof. Let $K \in \mathrm{Syl}_p\big(\mathrm{Fix}_G(\mathcal{B})\big)$, so $K \triangleleft G$.

Then $G \leq N_{S_p \wr S_p}(K)$, and $K_p \triangleleft N_{S_p \wr S_p}(K)$, so $G \leq N_{S_p \wr S_p}(K_p) = S_p \wr \mathrm{Aff}(1,p)$.

Because K is invariant under $\mathbb{Z}_p \wr e$, and the $\mathbb{Z}_p$-invariant subgroup of order p^i is unique, we know that K is normalized by $\mathrm{Aff}(1,p) \wr e$.

From the list of doubly transitive groups, we see that $\mathrm{Aff}(1,p)$ is maximal in S_p.

Therefore $N_{S_p \wr \mathrm{Aff}(1,p)}(K)/\mathcal{B} = S_{\mathcal{B}}$.

Then the following result of modular representation theory implies that $|K| \in \{1, p, p^{p-1}, p^p\}$.

Prop. *Let* $\chi\colon S_{p-1} \to \mathbb{Z}_p^*$ *be a homomorphism. Nontrivial invariant subspaces of* $\operatorname{Ind}_{S_{p-1}}^{S_p} \chi$ *have either dimension 1 or codimension 1.*

More generally, coding theorists have calculated the automorphism group of any code admitting $\mathrm{Aff}(d, q)$.

Lem. *Assume*

- $\mathrm{Fix}_G(\mathcal{B})$ *has a unique Sylow p-subgroup Q;*
- $\exp(P) = p^2$*; and*
- $|P| \neq p^{p+1}$

Then $P \triangleleft G$.

Proof. We have

$$\frac{G}{Q} \hookrightarrow \frac{(S_p \times \mathbb{Z}_p^*) \ltimes (\mathbb{Z}_p)^p}{K_{p-1}} \cong S_p \times \mathrm{Aff}(1,p)$$

Let $\phi\colon G/Q \to \mathrm{Aff}(1,p)$ (the projection).

WMA ϕ not faithful; else $G/\mathcal{B}$ solvable, so done.

$G/\mathcal{B}$ primitive $\Rightarrow \ker\phi$ transitive $\Rightarrow |\ker\phi|_p = p$; therefore, the image of ϕ is a p'-group.

Therefore, every p-element of G is in the kernel of ϕ, so $P \subset \mathbb{Z}_p \ltimes K_{p-1}$.

So every element of P has order p.

• M. Bardoe and P. Sin, The permutation modules for $\mathrm{GL}(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *London Math. Soc.* (to appear).

• P.J. Cameron, Finite Permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** 1981, 1-22.

• W. Feit, Some consequences of the classfication of finite simple groups, *Proc. Symp. Pure Math.* 37 (1980) 175–181. B. Cooperstein and G. Mason, eds, *The Santa Cruz Conference on Finite Groups*, Amer. Math. Soc., 1980.

• W. C. Huffman, Codes and Groups, in V.S. Pless and W.C. Huffman, eds., *Handbook of Coding Theory*, vol. 2, Elsevier, 1998, pp. 1345–1440.

• A. S. Kleshchev and A. A. Premet, On second degree cohomology of symmetric and alternating groups, *Comm. Alg.* 21(2) (1993) 583–600.

• B. Mortimer, The modular permutation representations of the known doubly transitive groups, *Proc. London Math. Soc.* (3) 41 (1980) 1–20.

• H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

• H. Wielandt, Permutation groups through invariant relations and invariant functions, in: B. Huppert and H. Schneider, eds., *Mathematische Werke = Mathematical Works / Helmut Wielandt*, vol. 1, de Gruyter, Berlin, 1994, pp. 237–296. QA3.W520.1994.V1 [Thm. 16.2, 16.3]