V finite dim. vector space over a field F

G acting linearly on V, then there is an induced action on $F[V]$

$$F[V]^G = \{ f \in F[V] \mid gf = f, \ \forall g \in G \}$$

Definition: A subset $X \subseteq F[V]^G$ is separating if $\forall x, y \in V$ we have

if $f(x) = f(y)$ $\forall f \in X$, then $f(x) = f(y)$ $\forall f \in F[V]^G$

Theorem (Derksen-Kemper, 2002) All invariant rings have finite separating sets.

(Derksen - Kemper, 2002)
- Noether bound holds for separating invariants in all characteristics

- (Draisma, Kemper, Wehlau) 2006
Weyl's polarization theorem holds for separating invariants in all characteristics

- (Domokos, 2007)
Further efficiency results on sep. invariants for decomposable representations.

Modular separating and generating Invariants

char $F = p$

$G = \mathbb{Z}/p^r$ has p^r indecomposable representations

$$V_i = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ \cdot & \cdot & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & 0 \\ 0 & 0 & 0 & \cdot \; 1 & 0 \\ 0 & 0 & 0 & \cdot \; 1 & 1 \end{pmatrix}_{i \times i} \qquad 1 \le i \le p^r$$

$F[V_2]^{\mathbb{Z}/p}$, $F[V_3]^{\mathbb{Z}/p}$ (Dickson 1913)

$F[V_4]^{\mathbb{Z}/p}$, $F[V_5]^{\mathbb{Z}/p}$ (Shank 1998)

$F[mV_2]^{\mathbb{Z}/p}$ (Campbell-Hughes, 1997)

$F[2V_3]^{\mathbb{Z}/p}$ (Campbell-Fodden-Wehlau, 2006)

$F[V_2 + V_3]^{\mathbb{Z}/p}$ (Shank-Wehlau, 2002)

$F[V_i]^{\mathbb{Z}/p}$ $i \le 9$, $F[W]^{\mathbb{Z}/p}$, where each indec. summand in W has dimension at most 4, (Wehlau, 2009)

(Fleischmann, M.S., Shank, Woodcock, 2006)
Exact degree required to generate $F[V]^{\mathbb{Z}/p}$ for any V is given.

$\mathbb{Z}/p^r \quad r>1$

i) $F[V_{p+1}]^{\mathbb{Z}/p^2}$ (Shank-Wehlau, 2005)

ii) $F[V_i]^{\mathbb{Z}/4^2}$ (Neusel, Sezer, 2008)
An infinite generating set is given: Norms, transfers and invariants up to some degree.

(Symonds, 2009) $F[V]^G$ is generated by invariants of degree at most

$$(\dim V)(|G|-1)$$

V, G arbitrary.

Separating Invariants

G any p-group.
$e_1, e_2, \dots, e_n$ be a basis for V^G
$x_1, x_2, \dots, x_n$ be the corresponding elements in V^*

(Newel, M.S) Subalgebra of $F[V]^G$ generated by $N(x_i)$ $1 \le i \le n$ and I is separating.

$$I = \sum_{H \text{ maximal}} \operatorname{Im} \operatorname{Tr}_H^G$$

<u>An Approach</u>:

We want to find a separating set for V.

Assume

$\pi : V \longrightarrow W$ G-equivariant surjection

and T is a separating set for W.

$F[W] \hookrightarrow F[V]$.

Say we want to separate $v_1, v_2 \in V$.
If $\pi(v_1)$ and $\pi(v_2)$ are in different orbits,
polynomial in T separates v_1, v_2.

Theorem: Let S be a separating set for V_{n-1}. Then S together with $N(x_n)$ and $Tr(x_n x_{i+1}^{p-1})$ $1 \leq i \leq n-2$ is a separating set for V_n.

How does this generalize to $\mathbb{Z}/p^r$?

$1 \leq i \leq n-2$ with $p^{k-1}+1 \leq n-i \leq p^k$

$G = \mathbb{Z}/p^r$ $\quad G_k = \mathbb{Z}/p^{r-k}$

$$H(i) = Tr_{G_k}^{G}\left(N_{G_k}(x_n) \prod_{0 \leq j \leq k-1} (N_{G_k}(x_{i+p^j}))^{p-1}\right)$$

Lemma: $H(i) \equiv N_{G_k}(x_n)\, x_i^{p^{r-k} \cdot k(p-1)} + f$ where $f \in F[x_1, x_2, \ldots, x_{n-1}]$ modulo $(x_{i-1}, \ldots, x_1)$

Theorem : $1 < n \leq p^r$

Let $S \subseteq F[V_{n-1}]^{\mathbb{Z}/p^r}$ be a separating set for V_{n-1}. then S together with $N_{\mathbb{Z}/p^r}(x_n)$ and $H(i)$ $1 \leq i \leq n-2$ is a separating set for V_n.