DICKSON INVARIANTS

STEVEN V SAM

Let q be a prime power, V a vector space of dimension n over the finite field $\mathbf{F}_q$, and $\mathbf{GL}(V)$ the group of invertible linear transformations on V. The goal of this note is to prove the following nice theorem of Dickson:

Theorem 1 (Dickson)**.** *The ring of invariants* $\mathrm{Sym}(V)^{\mathbf{GL}(V)}$ *is a polynomial algebra on n variables. The degrees of the generators are $q^n - q^i$ for $i = 0, \dots, n-1$. In particular, they are unique up to scalars.*

From the theorem, we see that these generators aren't stable under base change. For example, if we extend scalars to some finite extension of $\mathbf{F}_q$, these are no longer invariants (by looking at degrees). This is consistent with the fact that if we replaced $\mathbf{F}_q$ with its algebraic closure, then there are no non-constant invariants.

I'll follow the exposition in Wilkerson from `http://www.math.purdue.edu/~wilker/papers/dickson.pdf`, but I found the notation slightly confusing, so I'm going to change it.

Choose a basis $x_1, \dots, x_n$ for V. Let K be the field of fractions of $\mathrm{Sym}(V)$, i.e., $K = \mathbf{F}_q(x_1, \dots, x_n)$. Define a polynomial $f_n(t) \in K[t]$ by

$$f_n(t) = \prod_{\lambda \in V} (t - \lambda).$$

Lemma 2. *$f_n(t)$ can be written in the form*

$$f_n(t) = t^{q^n} + \sum_{i=0}^{n-1} c_{n,i} t^{q^i}$$

where $c_{n_i} \in \mathbf{F}_q[x_1, \dots, x_n]$ has degree $q^n - q^i$.

Proof. First consider the $(n+1) \times (n+1)$ matrix

$$M_n(t) = \begin{pmatrix} x_1 & x_2 & \cdots & x_n & t \\ x_1^q & x_2^q & \cdots & x_n^q & t^q \\ \vdots & & & & \\ x_1^{q^n} & x_2^{q^n} & \cdots & x_n^{q^n} & t^{q^n} \end{pmatrix}$$

and let $\Delta_n(t) = \det M_n(t)$. Note that $\Delta_n(\lambda) = 0$ whenever $\lambda \in V$ because $M_n(t)$ will have a linear dependency amongst its columns (since λ is a linear combination of the x_i). Since both $\Delta_n(t)$ and $f_n(t)$ are polynomials in t of degree q^n, and they have the same roots, we must have $\Delta_n(t) = c f_n(t)$ for some constant $c \in K$. But $f_n(t)$ is monic, and we can see that from the definition that the leading coefficient of $\Delta_n(t)$ is $\Delta_{n-1}(x_n)$, so $c = \Delta_{n-1}(x_n)$.

If $\Delta_{n-1}(t)$ is not identically 0, then all of its roots lie in the span of $\{x_1, \dots, x_{n-1}\}$, which implies that $\Delta_n(t)$ is not identically 0. Since $\Delta_1(t) = x_1 f_1(t) \neq 0$, we see that all of the $\Delta_n(t)$

Date: March 17, 2011.

are nonzero polynomials. Hence if we let C_i be the determinant of the submatrix of $M_n(t)$ obtained by deleting the last column and ith row, we see that $c_{n,i} = (-1)^{n-i} C_i / \Delta_{n-1}(x_n)$.

That $c_{n,i}$ is a polynomial in the x_i and has degree $q^n - q^i$ can be seen from the original definition of $f_n(t)$. Furthermore, $c_{n,i}$ is invariant under $\mathbf{GL}(V)$ because any change of basis can only scale $\Delta_n(t)$, and $\Delta_{n-1}(x_n)$ will also be scaled by the same amount. Also from the identity

$$\prod_{\lambda \in V} (t - \lambda) = t^{q^n} + \sum_{i=0}^{n-1} c_{n,i} t^{q^i},$$

we see that each $\lambda \in V \subset \mathrm{Sym}(V)$ satisfies a monic polynomial equation with coefficients in $R = \mathbf{F}_q[c_{n,0}, \ldots, c_{n,n-1}]$, so the same is true for all of $\mathrm{Sym}(V)$ by basic properties of integral extensions of rings. Passing to their fields of fractions $F(R)$ and $F(\mathrm{Sym}(V))$, we get an algebraic extension, and hence both of them have the same transcendence degree (namely, n) over $\mathbf{F}_q$. Since R is generated by n elements over $\mathbf{F}_q$, they must be algebraically independent (we hadn't even shown they were nonzero previously!), so that R is a polynomial ring. $\square$

All that remains to show is that we have found all of the invariants. Note that $F(\mathrm{Sym}(V))$ is the splitting field over $F(R)$ of the polynomial $f_n(t)$, so it is in fact a Galois extension. Let W be the Galois group. Since $\mathbf{GL}(V)$ leaves $F(R)$ pointwise fixed, we have $\mathbf{GL}(V) \subseteq W$. On the other hand, W permutes the roots of $f_n(t)$, i.e., W acts on V. Furthermore, W acts $\mathbf{F}_q$-linearly on V since W acts by field automorphisms on $F(\mathrm{Sym}(V))$, and since W fixes $\mathbf{F}_q$ pointwise. Hence $W \subseteq \mathbf{GL}(V)$ and hence we get equality $W = \mathbf{GL}(V)$.

This implies in particular that $F(\mathrm{Sym}(V))^{\mathbf{GL}(V)} = F(R)$, so that $\mathrm{Sym}(V)^{\mathbf{GL}(V)} \subset F(R)$. Finally, R is integrally closed (being a polynomial ring), and we have already seen that $\mathrm{Sym}(V)$ (and hence $\mathrm{Sym}(V)^{\mathbf{GL}(V)}$) is integral over R, so we conclude that $\mathrm{Sym}(V)^{\mathbf{GL}(V)} = R$.