BULL. AUSTRAL. MATH. SOC. 12F20, 20G05
VOL. 39 (1989) [107–117]

THE INVARIANTS OF PROJECTIVE LINEAR GROUP ACTIONS

HUAH CHU, MING-CHANG KANG AND ENG-TJIOE TAN

Let F_q be the field with q elements and let $G = PGL_n(F_q)$ or $PSL_n(F_q)$ act on $F_q(x_1, \ldots, x_{n-1})$, the rational function field of $n-1$ variables. Then $F_q(x_1, \ldots, x_{n-1})^G$ is purely transcendental over F_q. In fact, a set of $n-1$ generators of $F_q(x_1, \ldots, x_{n-1})^G$ over F_q is exhibited. The case $n = 2$ is treated by direct computation.

1. INTRODUCTION

Let F_q be the finite field with q elements, $F_q[x_1, \ldots, x_n]$ the polynomial ring in n variables over F_q, on which the n-dimensional general linear group $GL_n(F_q)$ over F_q acts naturally. In 1911, L.E. Dickson showed that the ring of invariants $F_q[x_1, \ldots, x_n]^{GL_n(F_q)}$ is again a polynomial ring on n generators (Dickson's invariants) [**1**, pp.80–84; **3**, pp.422–424].

As pointed out by Wilkerson [**3**, p.428], a crucial step in computing polynomial invariants in characteristic p is to make a good guess for a set of generators for the invariants. The ring of invariants $F_q[x_1, \ldots, x_n]^{SL_n(F_q)}$ of the special linear group was computed by this strategy.

It seems not to have been noticed that the projective linear groups $PGL_n(F_q)$, $PSL_n(F_q)$ should also be amenable to this strategy. For a field K containing F_q consider the following action of $PGL_n(F_q)$ on the rational function field $K(x_1, \ldots, x_{n-1})$ in $n-1$ variables. For each $\sigma \in PGL_n(F_q)$, choose a preimage $(a_{ij})_{1 \leqq i,j \leqq n}$ in $GL_n(F_q)$ and define, for $1 \leqq i \leqq n-1$,

$$\sigma \cdot x_i = \frac{a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{i,n-1}x_{n-1} + a_{in}}{a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{n,n-1}x_{n-1} + a_{nn}}.$$

Since $PSL_n(F_q)$ is a subgroup of $PGL_n(F_q)$, we consider the same action for $PSL_n(F_q)$ on $K(x_1, \ldots, x_{n-1})$.

In this note we confirm—as expected—the rationality of $K(x_1, \ldots, x_{n-1})^G$, $G = PGL_n(F_q)$ or $PSL_n(F_q)$ and *compute* explicitly the $n-1$ generators for their invariants (Theorem); in both cases the computation is reduced to a problem of finding a basis of a free-abelian group of rank $n-1$ in a free-abelian group of rank n (Lemma 2). This

Received 6 April, 1988
Partially supported by National Science Council, Republic of China, grant NSC. 77-0208-M002-31.

reduction process is based on the crucial observation that $K(x_1,\ldots,x_{n-1})^{PGL_n(F_q)}$ is the set of all degree zero elements of $K(y_1,\ldots,y_n)^{GL_n(F_q)}$, where $y_i = x_i y_n$, $1 \leqq i \leqq n-1$ (Lemma 1); the latter is completely known by Dickson's Theorem.

In Section 4 we try our hand (in the spirit of good guessing) at providing a "tour de force" process to compute a generator for $F_q(x)^{PSL_2(F_q)}$, using a different method. This process seems not to be straightforward, so we feel that it deserves to be mentioned in the literature.

2. The main results

Let K be a field containing F_q. We can embed $K(x_1,\ldots,x_{n-1})$ in a field $K(y_1,\ldots,y_n)$ in n variables over K by defining $x_i = \dfrac{y_i}{y_n}$ for $1 \leqq i \leqq n-1$. In fact, if we define the degree of $f \cdot g^{-1}$ by $\deg(f \cdot g^{-1}) = \deg f - \deg g$, where f, g are homogeneous polynomials in the polynomial ring $K[y_1, y_2, \ldots, y_n]$, then $K(x_1,\ldots,x_{n-1})$ is just the set of degree zero elements in $K(y_1,\ldots,y_n)$.

If we define the actions of $GL_n(F_q)$ and $SL_n(F_q)$ on $K[y_1,\ldots,y_n]$ by

$$\sigma \cdot y_i = a_{i1}y_1 + a_{i2}y_2 + \ldots + a_{in}y_n, \qquad 1 \leqq i \leqq n,$$

where $\sigma = (a_{ij})_{1 \leqq i,j \leqq n}$ is in $GL_n(F_q)$ or $SL_n(F_q)$, then the action of $PGL_n(F_q)$ or $PSL_n(F_q)$ on $K(x_1,\ldots,x_{n-1})$ is the induced action of $GL_n(F_q)$ or $SL_n(F_q)$ on $K(y_1,\ldots,y_n)$.

To formulate our main theorem we recall the definition of Dickson's invariants.

Let $\Delta_{n,n}$ be the $(n+1)\times n$ matrix whose (i, j)-th entry is $y_j^{q^{i-1}}$, for $1 \leqq i \leqq n+1$ and $1 \leqq j \leqq n$:

$$\Delta_{n,n} = \begin{bmatrix} y_1 & y_2 & \cdots & y_{n-1} & y_n \\ y_1^q & y_1^q & \cdots & y_{n-1}^q & y_n^q \\ \vdots & \vdots & & \vdots & \vdots \\ y_1^{q^n} & y_2^{q^n} & \cdots & y_{n-1}^{q^n} & y_n^{q^n} \end{bmatrix}.$$

Now let L_n be the determinant of the matrix obtained from $\Delta_{n,n}$ by deleting the $(n+1)$-th row. For $1 \leqq i \leqq n-1$, let $Q_{n,i}$ be the product of L_n^{-1} and the determinant of the matrix obtained from $\Delta_{n,n}$ by deleting the $(i+1)$-th row. Namely,

$$L_n = \det \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1^q & y_2^q & \cdots & y_n^q \\ \vdots & \vdots & & \vdots \\ y_1^{q^{n-1}} & y_2^{q^{n-1}} & \cdots & y_n^{q^{n-1}} \end{bmatrix}$$

$$Q_{n,i} = \det \begin{bmatrix} y_1 & y_2 & \dots & y_n \\ \vdots & \vdots & & \vdots \\ y_1^{q^{i-1}} & y_2^{q^{i-1}} & \dots & y_n^{q^{i-1}} \\ y_1^{q^{i+1}} & y_2^{q^{i+1}} & \dots & y_n^{q^{i+1}} \\ \vdots & \vdots & & \vdots \\ y_1^{q^n} & y_2^{q^n} & \dots & y_n^{q^n} \end{bmatrix} \cdot L_n^{-1}, \quad \text{for } 1 \leqq i \leqq n-1.$$

The following theorem of Dickson asserts that the rings of invariants of $K[y_1, \dots, y_n]$ under $GL_n(F_q)$ or $SL_n(F_q)$ action are still polynomial rings.

DICKSON'S THEOREM. [**1**, *pp.80–84*; **3**, *pp.422–424*]

(i) $$K[y_1, y_2, \dots y_n]^{GL_n(F_q)} = K[L_n^{q-1}, Q_{n,1}, Q_{n,2}, \dots, Q_{n,n-1}]$$

(ii) $$K[y_1, y_2, \dots, y_n]^{SL_n(F_q)} = K[L_n, Q_{n,1}, Q_{n,2}, \dots, Q_{n,n-1}].$$

We now dehomogenise the L_n and $Q_{n,i}$'s with respect to y_n to yield

$$\tilde{L}_n = \det \begin{bmatrix} x_1 & x_2 & \dots & x_{n-1} & 1 \\ x_1^q & x_2^q & \dots & x_{n-1}^q & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \dots & x_{n-1}^{q^{n-1}} & 1 \end{bmatrix}$$

$$\tilde{Q}_{n,i} = \det \begin{bmatrix} x_1 & x_2 & \dots & x_{n-1} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^{i-1}} & x_2^{q^{i-1}} & \dots & x_{n-1}^{q^{i-1}} & 1 \\ x_1^{q^{i+1}} & x_2^{q^{i+1}} & \dots & x_{n-1}^{q^{i+1}} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^n} & x_2^{q^n} & \dots & x_{n-1}^{q^n} & 1 \end{bmatrix} \cdot \tilde{L}_n^{-1}.$$

Our main result is the following:

THEOREM.

(i) $K(x_1, x_2, \dots, x_{n-1})^{PGL_n(F_q)} = K(u_1, u_2, \dots, u_{n-1})$ *where*

$$u_1 = \tilde{Q}_{n,1}^{\frac{q^n-1}{q-1}} \cdot \tilde{L}_n^{-q^n+q},$$

$$u_i = \tilde{Q}_{n,i} \cdot \tilde{Q}_{n,1}^{\frac{q^n-q^i}{q-1}} \cdot \tilde{L}_n^{-q^n+q^i} \qquad \text{for } 2 \leqq i \leqq n-1.$$

(ii) *Let* $d = g.c.d.(n, q-1) = g.c.d.\left(q^{n-1} + q^{n-2} + \dots + q + 1, q^n - q\right)$.

Choose any integers α and β such that

$$\alpha\left(q^{n-1}+q^{n-2}+\ldots+q+1\right)+\beta(q^n-q)=d.$$

Then

$$K(x_1,\ldots,x_{n-1})^{PSL_n(F_q)}=K(v_1,v_2,\ldots,v_{n-1})$$

where

$$v_1=\tilde{L}_n^{\frac{q^n-q}{d}}\cdot\tilde{Q}_{n,1}^{-\frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}}$$

$$v_i=\tilde{Q}_{n,i}\cdot\tilde{L}_n^{-\frac{\alpha\left(q^n-q^i\right)}{d}}\cdot\tilde{Q}_{n,1}^{-\frac{\beta\left(q^n-q^i\right)}{d}}\qquad \text{for } 2\leqq i\leqq n-1.$$

In both cases the invariant subfields are again purely transcendental over K.

3. The proof of the Theorem

As already mentioned in Section 2, $K(x_1,\ldots,x_{n-1})$ is the set of all degree zero elements in $K(y_1,\ldots,y_n)$. So the compatibility of the $PGL_n(F_q)$-action on $K(x_1,\ldots,x_{n-1})$ with the $GL_n(F_q)$-action on $K(y_1,\ldots,y_n)$ implies that $K(x_1,\ldots,x_{n-1})^{PGL_n(F_q)}$ is just the set of all degree zero elements of $K(y_1,\ldots,y_n)^{GL_n(F_q)}$; the latter is $K\left(L_n^{q-1},Q_{n,1},Q_{n,2},\ldots,Q_{n,n-1}\right)$ by Dickson's Theorem.

Each element in $K(x_1,\ldots,x_{n-1})^{PGL_n(F_q)}$ is of the form $f\cdot g^{-1}$, where f and g are both linear combinations over K of monomials

$$\begin{cases}\left(L_n^{q-1}\right)^{\gamma_0}(Q_{n,1})^{\gamma_1}\cdots(Q_{n,n-1})^{\gamma_{n-1}}\\ \gamma_0(q^n-1)+\gamma_1(q^n-q)+\ldots+\gamma_{n-1}\left(q^n-q^{n-1}\right)=m,\qquad \gamma_i\in\mathbb{N}\cup\{0\}.\end{cases}$$

Note that $\deg L_n^{q-1}=q^n-1$, $\deg Q_{n,i}=q^n-q^i$, for $1\leqq i\leqq n-1$.

Choose a fixed n-tuple $(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})$ with $a_i\geqq 0$ and $\sum_{0\leqq i\leqq n-1}\alpha_i\left(q^n-q^i\right)=m$. Then any monomial which may appear in f or g is of the form $\left(L_n^{q-1}\right)^{\alpha_0+\beta_0}(Q_{n,1})^{\alpha_1+\beta_1}\cdots(Q_{n,n-1})^{\alpha_{n-1}+\beta_{n-1}}$ with $\sum_{0\leqq i\leqq n-1}\beta_i\left(q^n-q^i\right)=0$. Note that β_i can be negative.

In f/g, divide both the denominator and the numerator by $\left(L_n^{q-1}\right)^{\alpha_0}(Q_{n,1})^{\alpha_1}\cdots(Q_{n,n-1})^{\alpha_{n-1}}$ to get the new denominator and numerator, which are K-linear combinations of monomials of the form

$$(*)\qquad\begin{cases}\left(L_n^{q-1}\right)^{\beta_0}(Q_{n,1})^{\beta_1}\cdots(Q_{n,n-1})^{\beta_{n-1}},\\ \sum_{0\leqq i\leqq n-1}\beta_i\left(q^n-q^i\right)=0,\qquad \beta_i\in\mathbb{Z}.\end{cases}$$

Thus we have proved the following:

LEMMA 1.

(i) $K(x_1,\dots,x_{n-1})^{PGL_n(F_q)}$ *is generated over* K *by monomials of the form* $(\star)$.

(ii) $K(x_1,\dots,x_{n-1})^{PSL_n(F_q)}$ *is generated over* K *by monomials of the form*

$$(\star\star)\qquad \begin{cases} (L_n)^{\gamma_0}(Q_{n,1})^{\gamma_1}\cdots(Q_{n,n-1})^{\gamma_{n-1}}, \\ \gamma_0\left(\frac{q_{n-1}}{q-1}\right)\sum\limits_{1\leqq i\leqq n-1}\gamma_i(q^n-q^i)=0, \qquad \gamma_i\in\mathbf{Z} \end{cases}$$

The proof of (ii) is similar to that of (i).

Due to Lemma 1 the proof of our theorem is reduced to finding a certain $n-1$ basis in the free abelian group $\mathbf{Z}^n$ (written additively) of rank n with free basis

$$e_0=\begin{cases} L_n^{q-1}, & \text{in the } PGL_2\text{-case} \\ L_n, & \text{in the } PSL_2\text{-case} \end{cases}, \qquad e_i=Q_{n,i}, \qquad 1\leqq i\leqq n-1.$$

So let $h_1,h_2\colon \mathbf{Z}^n\to\mathbf{Z}$ be defined by:

$$h_1(e_0)=q^n-1,$$
$$h_2(e_0)=\frac{q^n-1}{q-1} \qquad \text{and}$$
$$h_1(e_i)=h_2(e_i)=q^n-q^i, \qquad 1\leqq i\leqq n-1.$$

Our task is now to compute:

$$\text{Kernel}\,(h_1)=\{\sum_{i=0}^{n-1}\beta_ie_i\,|\,\sum_{i=0}^{n-1}\beta_i(q^n-q^i)=0\},$$

and

$$\text{Kernel}\,(h_2)=\{\sum_{i=0}^{n-1}\gamma_ie_i\,|\,\gamma_0\frac{q^n-1}{q-1}+\sum_{i=1}^{n-1}\gamma_i(q^n-q^i)=0\}.$$

LEMMA 2.

(i) $\text{Kernel}\,(h_1)$ *is a free abelian group of rank* $n-1$ *with basis*

$$-\frac{q^n-q}{q-1}e_0+\frac{q^n-1}{q-1}e_1$$

and

$$e_i+\frac{q^n-q^i}{q-1}e_1-\frac{q^n-q^i}{q-1}e_0 \qquad (2\leqq i\leqq n-1).$$

(ii) Kernel (h_2) *is a free abelian group of rank* $n-1$ *with basis*

$$\frac{q^n-q}{d}e_0-\frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}e_1$$

and

$$e_i-\frac{q^n-q^i}{d}(\alpha e_0+\beta e_1)\qquad(2\leqq i\leqq n-1)$$

where d, α, *and* β *are defined in Theorem (ii).*

PROOF: First we have Image $(h_j)=\text{g. c. d}\{h_j(e_i)|i=0,\ldots,n-1\}\mathbf{Z}$. Hence

$$\text{Image}\,(h_1)=(q-1)\mathbf{Z}$$

and

$$\text{Image}\,(h_2)=d\mathbf{Z},$$

where

$$d=\text{g. c. d}\{\frac{q^n-1}{q-1},\quad q^n-q^i,\quad 1\leqq i\leqq n-1\}$$

$$=\text{g. c. d}\{n,\quad q-1\}=\text{g. c. d}\{\frac{q^n-1}{q-1},\quad q^n-q\}.$$

Note that $h_1(e_0-e_1)=q-1$ and $h_2(\alpha e_0+\beta e_1)=d$. Thus we have

$$\mathbf{Z}^n=\text{Kernel}\,(h_1)\oplus\mathbf{Z}(e_0-e_1)$$

and

$$\mathbf{Z}^n=\text{Kernel}\,(h_2)\oplus\mathbf{Z}(\alpha e_0+\beta e_1),$$

where α, $\beta\in\mathbf{Z}$ are chosen such $\alpha\left(\frac{q^n-1}{q-1}\right)+\beta(q^n-q)=d$.

(i) Note that

$$e_0-\frac{q^n-1}{q-1}(e_0-e_1)=e_1-\frac{q^n-q}{q-1}(e_0-e_1).$$

So a set of n generators $\{e_i-\frac{q^n-q^i}{q-1}(e_0-e_1)|0\leqq i\leqq n-1\}$ of Kernel (h_1) yields the $n-1$ basis in (i).

(ii) In this case Kernel (h_2) has a set of n generators consisting of

$$e_0-\frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}(\alpha e_0+\beta e_1)$$

and

$$e_i-\frac{q^n-q^i}{d}(\alpha e_0+\beta e_1)\qquad(1\leqq i\leqq n-1).$$

However, note that

$$e_0 - \frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}(\alpha e_0+\beta e_1)$$
$$= \beta\left(\frac{q^n-q}{d}e_0 - \frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}e_1\right)$$

and

$$e_1 - \frac{q^n-q}{d}(\alpha e_0+\beta e_1)$$
$$= -\alpha\left(\frac{q^n-q}{d}e_0 - \frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}e_1\right),$$

with α and β being relatively prime. It follows that the above two elements generate the cyclic subgroup whose generator is

$$\frac{q^n-q}{d}e_0 - \frac{q^{n-1}+q^{n-2}+\ldots+q+1}{d}e_1$$

and one gets the $n-1$ basis in (ii). This completes the proof of Lemma 2. ∎

Finally, define $u_1, u_2, \ldots, u_{n-1}$ and $v_1, v_2, \ldots, v_{n-1}$ as in the Theorem.

It is easy to see that any monomial of the form $(\star)$ and $(\star\star)$ of Lemma 1 can be written as a monomial in $u_1, u_2, \ldots, u_{n-1}$ and $v_1, v_2, \ldots, v_{n-1}$ respectively. Hence Lemma 1 and Lemma 2 complete the proof of our Theorem. ∎

4. The case $n = 2$

The case $n = 2$ can be computed directly without referring to Dickson's invariants. Note that $PSL_n(F_q) = PGL_n(F_q)$ if q is even. The proofs, which we will sketch briefly for $K = F_q$ and the PSL_2 case, are tedious and computational. They involve some mod p combinatorial identities that seem not to be straightforward. We feel that the computation is worth recording in the literature.

Our direct computation leads us to the following generators for the invariant fields.

(i) $F_q(x)^{PGL_2(F_q)} = F_q(t_1)$, where

$$t_1 = (x^q - x)^{-(q^2-q)}\{1 + (x^q-x)^{q-1} + (x^q-x)^{q^2-1}\}. \tag{1}$$

(ii) If q is odd, $F_q(x)^{PSL_2(F_q)} = F_q(t_2)$, where

$$t_2 = (x^q - x)^{-\frac{q^2-q}{2}}\{1 + (x^q-x)^{q-1}\}^{\frac{q+1}{2}}. \tag{2}$$

An alternative form for the formulae (1) and (2) is:

$$(1') \qquad t_1 = \frac{1 + z_1 + z_1^2 + \ldots + z_1^{q^2+q}}{z_1^q + z_1^{2q} + \ldots + z_1^{q^2}}, \qquad z_1 = x^{q-1}$$

and

$$(2') \qquad t_2 = \frac{\left(1 + z_2^2 + z_2^4 + \ldots + z_2^{2q}\right)^{\frac{q+1}{2}}}{z_2^q\left(z_2^{2q} - 1\right)^{\frac{q-1}{2}}}, \qquad z_2 = x^{\frac{q-1}{2}}.$$

By an easy calculation our generators (1) and (2) are, as expected, the correct ones

$$u_1 = t_1 + 1 \text{ and } v_1 = (-1)^{\frac{q-1}{2}} t_2^{-1}.$$

We might remark that a special case of the above results appears as an exercise in the first edition of Jacobson [2, Exercise 6, p.236].

In the rest of this section we indicate the steps by which we arrived at the correct generators t_1 and t_2.

Step 1. By analysis of the group action we obtain generators $\tilde{t}_1$ and $\tilde{t}_2$:

(i) $F_q(x)^{PGL_2(F_q)} = F_q(\tilde{t}_1)$, where

$$\tilde{t}_1 = (x^q - x)^{q-1}\{1 + \sum_{b \in F_q} (x+b)^{-(q^2-1)}\}.$$

(ii) If q is odd, $F_q(x)^{PSL_2(F_q)} = F_q(\tilde{t}_2)$, where

$$\tilde{t}_2 = (x^q - x)^{\frac{q-1}{2}}\{1 + \sum_{b \in F_q} (x+b)^{-\frac{q^2-1}{2}}\}.$$

PROOF: First note that

$$PGL_2(F_q) = \langle x \mapsto ax + c, x \mapsto \frac{a}{x+b} + c \mid a \in F_q\backslash\{0\} \ \& \ b, c \in F_q \rangle$$

$$PSL_2(F_q) = \langle x \mapsto a^2x + c, x \mapsto \frac{-a^2}{x+b} + c \mid a \in F_q\backslash\{0\} \ \& \ b, c \in F_q \rangle.$$

It is easily seen that $w = (x^q - x)^{\frac{q-1}{2}}$ is invariant under $H = \langle x \mapsto a^2x + c \mid a \in F_q\backslash\{0\}, c \in F_q \rangle$ and the orbit of w under $\langle x \mapsto -\frac{1}{x+b} \mid b \in F_q \rangle$ is $\{w, w(x+b)^{-\frac{q^2-1}{2}} | b \in F_q\}$. Moreover, $\sum_{b \in F_q} (x+b)^{-\frac{q^2-1}{2}}$ is invariant under H. Hence

$$\tilde{t}_2 = w\{1 + \sum_{b \in F_q} (x+b)^{-\frac{q^2-1}{2}}\}$$

is invariant under $PSL_2(F_q)$. Evaluating the degree $[F_q(x): F_q(\tilde{t}_2)] = \dfrac{q(q^2-1)}{2} = |PSL_2(F_q)|$ yields the assertion. ∎

Step 2. Evaluation of the sum in the curly brackets on the right-hand-side yields:

$$\sum_b (x+b)^{-(q^2-1)} = \sum_{1 \leqq j \leqq q} (-1)^{j+1} \binom{q-2+j(q-1)}{q-j} (x^q - x)^{-(q-1)(j+1)}.$$

If q is odd,

$$\sum_b (x+b)^{-\frac{q^2-1}{2}} = \sum_{0 \leqq j \leqq \frac{q-1}{2}} (-1)^{\frac{q-1}{2}-j} \binom{q-2+j(q-1)}{\frac{q-1}{2}-j} (x^q - x)^{-(q-1)(j+1)}.$$

PROOF: Set $s_n = \sum_{b \in F_q} (x+b)^n$. We evaluate the formula using the generating function of s_n

$$s_1 + s_2 T + s_3 T^2 + \ldots + s_{n+1} T^n + \ldots,$$

which has the following final form

$$-\{\frac{1}{x^q - x} + \frac{1}{(x^q - x)^2}(T^q - T) + \frac{1}{(x^q - x)^3}(T^q - T)^2 + \ldots + \frac{1}{(x^q - x)^{n+1}}(T^q - T)^n + \ldots\}.$$

We omit the explicit calculation and just note that we use the following identity:

$$\prod_{b \in F_q} \{T - (x+b)\} = (T-x)^q - (T-x) = T^q - T - (x^q - x)$$

Comparing the coefficients of $T^{\frac{q^2-3}{2}}$ yields the desired formula. ∎

Step 3. From Step 1 and Step 2 we have

$$\tilde{t}_2 = (x^q - x)^{-\frac{q^2-q}{2}} \{(x^q - x)^{\frac{q^2-1}{2}} + \sum_{0 \leqq j \leqq \frac{q-1}{2}} (-1)^{\frac{q-1}{2}-j} \times \binom{q-2+j(q-1)}{\frac{q-1}{2}-j} (x^q - x)^{\frac{q^2-1}{2}-(q-1)(j+1)}\}.$$

Let $k = \frac{q-1}{2} - j$ and $w = (x^q - x)^{q-1}$. The term in the curly brackets is

$$\sum_{0 \leqq k \leqq \frac{q-1}{2}} (-1)^k \binom{\frac{q^2-3}{2} - k(q-1)}{k} w^k + w^{\frac{q+1}{2}}.$$

We claim that the following holds, for each $0 \leqq k \leqq \frac{q-1}{2}$:

$$\text{(P)}\quad (-1)^k \binom{\frac{q^2-3}{2} - k(q-1)}{k} \equiv \binom{\frac{q+1}{2}}{k} \pmod{p}, \text{(where } q \text{ is a power of } p)$$

so that

$$\tilde{t}_2 = (x^q - x)^{-\frac{q^2-q}{2}} \{ \sum_{0 \leqq k \leqq \frac{q-1}{2}} \binom{\frac{q+1}{2}}{k} w^k + w^{\frac{q+1}{2}} \}$$

$$= (x^q - x)^{-\frac{q^2-q}{2}} \{(x^q - x)^{q-1} + 1\}^{\frac{q+1}{2}} = t_2$$

as was to be proved. (The computation for t_1 is analogous).

PROOF: To prove (P) we need the following mod p combinatorial identity:

$$\text{If } a = a_0 + a_1 q + \ldots + a_r q^r \text{ and}$$
$$b = b_0 + b_1 q + \ldots + b_r q^r$$

with $0 \leqq a_i, b_i \leqq q-1$ then

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_r}{b_r} \pmod{p}.$$

Here we adopt the following conventions: (i) $\binom{c}{d} = 0$ if $c < d$; (ii) $\binom{c}{0} = 1$ for any nonnegative integer c.

Now for $0 \leqq k \leqq \frac{q-1}{2}$ we have

$$\frac{q^2-3}{2} - k(q-1) = \left(\frac{q-1}{2} - k\right)q + \left(\frac{q-3}{2} + k\right),$$

hence

$$\binom{\frac{q^2-3}{2} - k(q-1)}{k} \equiv \binom{\frac{q-1}{2} - k}{0} + \binom{\frac{q-3}{2}}{k} \pmod{p}.$$

By direct check we have $\binom{\frac{q-3}{2} + k}{k} \equiv \binom{\frac{q+1}{2}}{k} \pmod{p}$. This completes the proof of (P) and hence of Step 3. ∎

References

[1] L.E. Dickson, 'A fundamental system of invariants of the general modular linear group with a solution of the form problem', *Trans. Amer. Math. Soc.* **12** (1911), 75–98.

[2] N. Jacobson, *Basic Algebra I* (W.H. Freeman, San Francisco, 1974).

[3] C. Wilkerson, 'A primer on the Dickson invariants', in *Proc. of the Northwestern Homotopy Theory Conference* **19**: *Contemp. Math.*, pp. 421–434 (Amer. Math. Soc., Providence, R.I., 1983).

Dr H. Chu,
Department of Mathematics,
National Taiwan University,
Taipei, Taiwan, 10764
Republic of China

Professor M-C. Kang,
Department of Mathematics,
National Taiwan University,
Taipei, Taiwan, 10764
Republic of China

Dr E-T. Tan,
Department of Mathical Sciences,
National Chengchi University,
Mucha,
Taipei, Taiwan, 11623
Republic of China