MODULAR SUMS OF SQUARES

by

Pablo A. Acosta Solarte & Víctor S. Albis[1]

Resumen

Pablo A. Acosta Solarte & Víctor S. Albis: Modular sums of squares. Rev. Acad. Colomb. Cienc. **25**(97): 553-562, 2001. ISSN 0370-3908.

Se calcula el número de soluciones en $[K[X]/(p(X)^r)]^s = L_r^s$ de las ecuaciones $Q_r(t_1, \dots, t_s) = \alpha_1(z_r)t_1^2 + \dots + \alpha_s(z_r)t_s^2 = \beta(z_r)$, de coeficientes en L_r y se calcula la correspondiente serie de Poincaré.

Palabras clave: Sumas de cuadrados, series de Poincaré, formas cuadráticas.

Abstract

The number of solutions in $[K[X]/(p(X)^r)]^s = L_r^s$ of equations of the form $Q_r(t_1, \dots, t_s) = \alpha_1(z_r)t_1^2 + \dots + \alpha_s(z_r)t_s^2 = \beta(z_r)$, with coefficients in L_r is evaluated. The corresponding Poincaré series are also evaluated.

Key words: Sums of squares, Poincaré series, quadratic forms.

1. Introduction

The aim of this paper is to count the number of solutions of equations of the form $Q_r(t_1, \dots, t_s) = \alpha_1(z_r)t_1^2 + \dots + \alpha_s(z_r)t_s^2 = \beta(z_r)$, where $\alpha_i(z_r)$ $(i = 1, \dots, s)$, and $\beta(z_r)$ belong to certain finite $L-$algebras L_r (see *infra*). If each $\alpha_i = 1$, this amounts to count the number of ways an element $\beta(z_r)$ in L_r can be written as a sum of squares in L_r. This is the content of the second section. In the third Section we use these results to evaluate the Poincaré series (see *infra*) of $Q_r(t_1, \dots, t_s) = \beta(z_r)$.

The results in the second section extend the classical ones for finite fields contained in L. E. Dickson celebrated book [**3**]. The notations that we will use are those introduced in [**1**] and [**2**].

Let thus K be a finite field with q elements, and let $p(X)$ be a monic irreducile polynomial in $K[X]$ of degree m. Then it is known that $K[X]/(p(X)) = L$

[1]Departamento de Matemáticas y Estadística, Universidad Nacional de Colombia. Apartado aéreo 95480, Bogotá D. C., Colombia. e-mail: valbis@accefyn.org.co . Parcialmente asupiciado por el Contrato 089-2000 de COLCIENCIAS-UNAB.

is a finite field containing K and such that the dimension of the extension L/K is equal to the degree of the polynomial $p(X)$. Thus L is a field with q^m elements. We will write $\alpha(z_r)$ for the elements of $K[X]/(p(X)^r) = L_r$, $r = 1, 2, \ldots$. It is shown in [**1**] and [**2**] that $K[X]/(p(X)^r) = L_r$ is a K-algebra with q^{rm} elements and that

$$L_r = \{\alpha(z_r) = \alpha_0 + \alpha_1 z_r + \cdots + \alpha_{r-1} z_r^{r-1} : \alpha_i \in L\} ,$$

where $z_r^i \neq 0$ if $i = 0, 1, \ldots, r-1$ are all different, and $z_r^j = 0$ if $j \geq r$. In fact, 1, z_r, $\ldots$, z_r^{r-1} is a basis of the $K-$álgebra L_r. Its $L-$dimension is thus r.

If $r \leq v$, the mapping $\pi_{r,v} : L_v \to L_r$ defined by $\pi_{r,v}(\alpha(z_v)) = \alpha(z_r)$ is a homomorphism of $L-$algebras.

If $H_v(t_1, \ldots, t_s) \in L_v[t_1, \ldots, t_s]$ is a polynomial with coefficients in L_v and s indeterminates, then

$$\pi_{r,v}(H_v(t_1, \ldots, t_s)) = H_r(t_1, \ldots, t_s)$$

is the polynomial in $L_r[t_1, \ldots, t_s]$, whose coefficientes are the classes modulus $(p(X)^r)$ of the coefficients of $H_v(t_1, \ldots, t_s)$.

If $\boldsymbol{\tau}_v \in L_v^s$ is a zero of $H_v(t_1, \ldots, t_s)$, and $r \leq v$, we say that $\boldsymbol{\tau}_v$ is a *descendant* of $\boldsymbol{\tau}_r$ if $\pi_{r,v}(\boldsymbol{\tau}_v) = \boldsymbol{\tau}_r$. In this case we have $H_r(\boldsymbol{\tau}_r) = 0$. We also will say that $\boldsymbol{\tau}_r$ is an *ascendant* of $\boldsymbol{\tau}_v$.

A zero $\boldsymbol{\tau}_r \in L_r^s$ of H_r is said to be *regular* (or *non singular*) if

$$\frac{\partial H_1(\pi_{1,r}(\boldsymbol{\tau}_r))}{\partial t_j} = \frac{\partial H_1(\tau_{1,1}, \ldots, \tau_{1,s})}{\partial t_j} \neq 0 ,$$

for some $j = 1, \ldots, s$. Otherwise it is said to be *singular*.

Every descendant of a regular zero is regular. Indeed, since

$$\pi_{1,n}\left(\pi_{n,m}\left(\frac{\partial H_m(t_1, t_2, \ldots, t_s)}{\partial t_j}\right)\right) = \frac{\partial H_1(t_1, t_2, \ldots, t_s)}{\partial t_j} ,$$

we see that if $\boldsymbol{\tau}_n$ is regular zero and $\boldsymbol{\tau}_m$ is a descendant of $\boldsymbol{\tau}_n$, i.e., if $\boldsymbol{\tau}_n = \pi_{n,m}(\boldsymbol{\tau}_m)$ then

$$0 \neq \frac{\partial H_1(\pi_{1,n}(\boldsymbol{\tau}_n))}{\partial t_j} = \frac{\partial H_1(\pi_{1,n}(\pi_{n,m}(\boldsymbol{\tau}_m)))}{\partial t_j} = \frac{\partial H_1(\pi_{1,m}(\boldsymbol{\tau}_m))}{\partial t_j} ,$$

for some j.

As in [**2**], we denote by $c(r, H)$ the number of zeroes of H_r in L_r^s and by $d(r, \boldsymbol{\tau}_1)$ the number of descendants of $\boldsymbol{\tau}_1$ in L_r^s, where $\boldsymbol{\tau}_1$ is a zero of H_1 en L^s. It is easy to see that

$$c(r, H) = \sum_{\substack{\tau_1 \\ \text{zero of } H_1}} d(r, \boldsymbol{\tau}_1) . \tag{1}$$

A form $H_r(t_1, \ldots, t_s) \in L_r[t_1, \ldots, t_s]$ is said to be an *strongly non-degenerate form* if $(0, \ldots, 0) \in L^s$ is the unique singular zero of $H_1(t_1, \ldots, t_s)$. In particular, if the characteristic of K is different from 2 and the discriminat $\operatorname{disc} Q_1$ of the quadratic form $Q_1(t_1, \ldots, t_s) \in L[t_1, \ldots, t_s]$ is not zero, then the quadratic form

$$Q_r(t_1, \ldots, t_s) = \alpha_1(z_r)t_1^2 + \ldots + \alpha_s(z_r)t_s^2 \tag{2}$$

is strongly non-degenerate. In this case, a descendant of $\boldsymbol{\tau}_0 = (0, \ldots, 0)$ in L_r^s has the form

$$\boldsymbol{\tau}_r = \left(z_r \sum_{i=1}^{r-1} \tau_{1,i} z_r^{i-1}, \ldots, z_r \sum_{i=1}^{r-1} \tau_{s,i} z_r^{i-1}\right) ,$$

and thus

$$Q_r(\boldsymbol{\tau}_r) = z_r^2 Q_r\left(\sum_{i=1}^{r-1} \tau_{1,i} z_r^{i-1}, \ldots, \sum_{i=1}^{r-1} \tau_{s,i} z_r^{i-1}\right) . \tag{3}$$

If $r \leq 2$, then (3) is always equal to zero. Therefore $d(2; \boldsymbol{\tau}_0) = q^{ms}$. If $r > 2$, the equation (3) is equal to zero if, and only if,

$$Q_{r-2}\left(\sum_{i=1}^{r-2} \tau_{1,i} z_{r-2}^{i-1}, \ldots, \sum_{i=1}^{r-2} \tau_{s,i} z_{r-2}^{i-1}\right) = 0 ,$$

by virtue of proposition 2.4 of [**2**]. Consequently,

$$d(r; \boldsymbol{\tau}_0) = c(r-2) q^{2ms} . \tag{4}$$

From now on all the fields considered are supposed to be of characteristic $p \neq 2$.

Let $Q(t_1, \ldots, t_s) = a_1 t_1^2 + \cdots + a_s t_s^2$ be a quadratic form with coefficients in the finite field $\mathbb{F}_q$ whose characteristic is not 2. We define, for $s = 2m$ or $s = 2m + 1$,

$$\nu(a_1, \ldots, a_s) = \nu_Q := \begin{cases} 1 & \text{si } (-1)^m \operatorname{disc} Q \in {\mathbb{F}_q}^{\times 2} , \\ -1 & \text{si } (-1)^m \operatorname{disc} Q \notin {\mathbb{F}_q}^{\times 2} . \end{cases}$$

We denote by $N(Q, q, b)$ the number of solutions of the equation

$$Q(t_1, \ldots, t_s) = a_1 t_1^2 + \cdots + a_s t_s^2 = b ,$$

$(b \in \mathbb{F}_q)$ in ${\mathbb{F}_q}^s$.

The following results are proved in [**3**, pp. 46–48]:

Proposition 1.1. *Let* $Q(t_1, \ldots, t_s) = a_1t_1^2 + \cdots + a_st_s^2$, $s = 2m$, *be a quadratic form with* $\operatorname{disc} Q \neq 0$. *Then*

$$N(Q, q, b) = \begin{cases} q^{2m-1} - \nu_Q q^{m-1} & \text{if } b \neq 0\,, \\ q^{2m-1} + \nu_Q(q^m - q^{m-1}) & \text{if } b = 0\,. \end{cases}$$

Proposition 1.2. *Let* $Q(t_1, \ldots, t_s) = a_1t_1^2 + \cdots + a_st_s^2$, $s = 2m + 1$, *be a quadratic form with* $\operatorname{disc} Q \neq 0$. *Then*

$$N(Q, q, b) = q^{2m} + \omega(b, a_1, \ldots, a_{2m+1})q^m\,,$$

where

$$\omega(b, a_1, \ldots, a_{2m+1}) = \begin{cases} 1 & \text{if } (-1)^m b \operatorname{disc} Q \in \mathbb{F}_q^{\times 2}, \\ -1 & \text{if } (-1)^m b \operatorname{disc} Q \notin \mathbb{F}_q^{\times 2}, \\ 0 & \text{if } (-1)^m b \operatorname{disc} Q = 0\,. \end{cases}$$

2. Modular sums of squares

In order to prove the main results in this section we will need the following lemmata.

Lemma 2.1. *Let* $Q_r(t_1, \ldots, t_s) \in L_r[t_1, \ldots, t_s]$ *be a strongly non-degenerated quadratic form. Then the number of solutions* $N_R(r, Q)$ *of* $Q_r(t_1, \ldots, t_s) = 0$ *which are descendants of the regular zeroes of* Q_1 *is given by*

$$\left[q^{m(2u-1)} + \nu_{Q_1}(q^{mu} - q^{m(u-1)}) - 1\right]q^{(r-1)m(s-1)}$$

if $s = 2u$, *and by*

$$\left[q^{2mu} - 1\right]q^{(r-1)m(s-1)}$$

if $s = 2u + 1$.

Proof. Let $\boldsymbol{\tau}_1 \in L^s$ be a non-trivial zero of the given quadratic form $Q_1(t_1, \ldots, t_s)$. By [**2**, proposition 2.5, and its proof] this zero always has descendants, and by recurrence we obtain

$$\begin{aligned} d(1, \boldsymbol{\tau}_1) &= 1 \\ d(2, \boldsymbol{\tau}_1) &= d(2-1, \boldsymbol{\tau}_1)q^{m(s-1)} = q^{m(s-1)} \\ &\cdots \\ d(r, \boldsymbol{\tau}_1) &= d(r-1, \boldsymbol{\tau}_1)q^{m(s-1)} = \ldots = q^{(r-1)m(s-1)}. \end{aligned}$$

Using (1) and propositions 1.1 y 1.2, we see that $N_R(r, Q)$ is given by

$$[c(1, H) - 1]q^{(r-1)m(s-1)} = \left[q^{m(2u-1)} + \nu_{Q_1}(q^{mu} - q^{m(u-1)}) - 1\right]q^{(r-1)m(s-1)}$$

when $s = 2u$, and by

$$N_R(r, Q) = [c(1, H) - 1]q^{(r-1)m(s-1)} = \left[q^{2mu} - 1\right]q^{(r-1)m(s-1)}$$

when $s = 2u + 1$. □

Lemma 2.2. *Let* $Q_r(t_1, \ldots, t_s) \in L_r[t_1, \ldots, t_s]$ *be a strongly non-degenerate quadratic form. Then the number* $N_S(r, Q)$ *of solutions which descend from* $\boldsymbol{\tau}_0 = (0, .., 0)$ *of* $Q_r(t_1, \ldots, t_s) = 0$ *is given by*

$$q^{(r-1)ms} + [c(1, Q) - 1]\frac{q^{(r-2)m(s-1)} - q^{(r-2)ms}}{q^{2m(s-1)} - q^{2ms}}q^{m(s-1)}q^{2ms}$$

if r *is even, and by*

$$c(1, Q)q^{(r-1)ms} + [c(1, Q) - 1] \times \frac{q^{(r-3)m(s-1)} - q^{(r-3)ms}}{q^{2m(s-1)} - q^{2ms}}q^{2m(s-1)}q^{2ms},$$

if r *is odd.*

Proof. Accordingly to the results in section 1, the number of descendants of $\tau_0 = (0, \ldots, 0)$ is given by

$$d(1,\tau_0) = 1$$
$$d(2,\tau_0) = q^{ms}$$
$$d(3,\tau_0) = c(1,Q)q^{2ms}$$
$$d(4,\tau_0) = c(2,Q)q^{2ms} = \left(d(2,\tau_0) + [c(1,Q)-1]q^{m(s-1)}\right)q^{2ms} = q^{3ms} + [c(1,Q)-1]q^{m(s-1)}q^{2ms}$$
$$d(5,\tau_0) = c(3,Q)q^{2ms} = \left(d(3,\tau_0) + [c(1,Q)-1]q^{2m(s-1)}\right)q^{2ms} = c(1,Q)q^{4ms} + [c(1,Q)-1]q^{2m(s-1)}q^{2ms}$$
$$d(6,\tau_0) = c(4,Q)q^{2ms} = \left(d(4,\tau_0) + [c(1,Q)-1]q^{3m(s-1)}\right)q^{2ms} = q^{5ms} + [c(1,Q)-1]\left(q^{3m(s-1)}q^{2ms} + q^{m(s-1)}q^{4ms}\right)$$
$$d(7,\tau_0) = c(5,Q)q^{2ms} = \left(d(5,\tau_0) + [c(1,Q)-1]q^{4m(s-1)}\right)q^{2ms}$$
$$= c(1,Q)q^{6ms} + [c(1,Q)-1]\left(q^{4m(s-1)}q^{2ms} + q^{2m(s-1)}q^{4ms}\right)$$
$$\ldots$$

Thus,

$$d(r,\tau_0) = q^{(r-1)ms} + [c(1,Q)-1]\left(q^{(r-3)m(s-1)}q^{2ms} + q^{(r-5)m(s-1)}q^{4ms} + \ldots + q^{3m(s-1)}q^{(r-4)ms} + q^{m(s-1)}q^{(r-2)ms}\right)$$
$$= q^{(r-1)ms} + [c(1,Q)-1]\left(\frac{q^{(r-2)m(s-1)} - q^{(r-2)ms}}{q^{2m(s-1)} - q^{2ms}}q^{m(s-1)}q^{2ms}\right),$$

if r is even, and

$$d(r,\tau_0) = c(1,Q)q^{(r-1)ms} + [c(1,Q)-1]\left(q^{(r-3)m(s-1)}q^{2ms} + q^{(r-5)m(s-1)}q^{4ms} + \cdots + q^{4m(s-1)}q^{(r-5)ms} + q^{2m(s-1)}q^{(r-3)ms}\right)$$
$$= c(1,Q)q^{(r-1)ms} + [c(1,Q)-1]\left(\frac{q^{(r-3)m(s-1)} - q^{(r-3)ms}}{q^{2m(s-1)} - q^{2ms}}q^{2m(s-1)}q^{2ms}\right),$$

if r is odd. □

Proposition 2.1. *Let $Q_r(t_1, \ldots, t_s) \in L_r[t_1, \ldots, t_s]$ be strongly non-degenerate quadratic form. Then the number of solutions $c(r,Q)$ of $Q_r = 0$ is given by*

$$c(r,Q) = N_R(r,Q) + N_S(r,Q)$$

Proof. We know that

$$c(r,Q) = \sum_{\substack{\tau_1 \\ \text{zero of } Q_1}} d(r,\tau_1)$$

and since Q_1 has only one singular zero, namely $\tau_0 = (0, \ldots, 0)$, then

$$c(r,Q) = d(r,\tau_0) + \sum_{\substack{\tau_1 \neq \tau_0 \\ \text{zero of } Q_1}} d(r,\tau_1)$$
$$= N_S(r,Q) + N_R(r,Q).$$ □

Next, we consider the equation

$$Q_r(t_1, \ldots, t_s) = \alpha_1(z_r)t_1^2 + \ldots + \alpha_s(z_r)t_s^2 = \beta(z_r). \quad (5)$$

Thus in L, we have the equation

$$\alpha_1(z)t_1^2 + \ldots + \alpha_s(z)t_s^2 = \beta(z). \quad (6)$$

If $\beta(z) = 0$ we refer to proposition 2.1. So we may, without lost of generality, suppose now that $\beta(z_r) \neq 0$. In this case it is clear that $(0, \ldots, 0)$ is not a solution of (6), so all of its solutions are non singular. Using propositions 1.1 and 1.2, the number of solutions of (6) in L^s is given by

$$q^{m(s-1)} - \nu_{Q_1}q^{m(u-1)},$$

if $s = 2u$. Since all of them are non singular, for each one of them the number of its descendants in L_r^s is $q^{m(r-1)(s-1)}$. Therefore (5) has

$$q^{m(r-1)(s-1)}\left(q^{m(2u-1)} - \nu_{Q_1}q^{m(u-1)}\right)$$

solutions. If $s = 2u+1$, (6) has

$$q^{2mu} + \omega(\beta(z), \alpha_1(z), \ldots, \alpha_s(z))q^{mu}$$

solutions, in L^s. Therefore,

$$q^{m(r-1)(s-1)}\left(q^{2mu}+\omega(\beta(z),\alpha_1(z),\dots,\alpha_s(z))q^{mu}\right)$$

is the number of solutions of (5) in L_r^s. Thus we have proved the following result:

Proposition 2.2. *Let $Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2$ be a strongly non-degenerate form in $L_r[t_1,\dots,t_s]$. Then the number of solutions of*

$$Q_r(t_1,\dots,t_s)=\beta(z_r),\qquad \beta(z)\neq 0\ ,$$

in L_r^s is given by

$$q^{m(r-1)(s-1)}\left(q^{m(2u-1)}-\nu_{Q_1}q^{m(u-1)}\right)$$

if $s=2u$ and by

$$q^{m(r-1)(s-1)}\left(q^{2mu}+\omega(\beta(z),\alpha_1(z),\dots,\alpha_s(z))q^{mu}\right)$$

if $s=2u+1$. □

Let us suppose now that the quadratic form is not strongly non-degenerate in $L_r[t_1,\dots,t_s]$. This means that if

$$Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2\ ,$$

is in $L_r[t_1,\dots,t_s]$, then

$$Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2+0t_{v+1}^2+\dots+0t_s^2\ ,$$

where $v<s$ (assuming the indicated order without loss of generality).

In this case $(0,\dots,0)\in L^s$ is not the only singular zero of Q_1, since $(0,\dots,0)\in L^v$ can be completed in $q^{m(s-v)}$ ways to a singular zero (also the regular zeroes can be completed in a similar way) in L^s. Using (1), and propositions 1.1 and 1.2, and the preceeding remarks we conclude that the value of $c(1,Q)$ is given by

$$\left[q^{m(2u-1)}+\nu(\alpha_1,\dots,\alpha_v)(q^{mu}-q^{m(u-1)})\right]q^{m(s-v)}\qquad(7)$$

when $v=2u$, and

$$q^{2mu}q^{m(s-v)}\qquad(8)$$

when $v=2u+1$, where we have written α_i instead of $\alpha_i(z)$.

Lemma 2.3. *Let $Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2\in L_r[t_1,\dots,t_s]$ be such that $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2$ in $L[t_1,\dots,t_s]$, with $v<s$. Then $N_R(r,Q)$ is given by*

$$\left[q^{m(2u-1)}+\nu_{Q_1}(q^{mu}-q^{m(u-1)})-1\right]q^{m[(r-1)(s-1)+(s-v)]}$$

if $v=2u$, and by

$$\left[q^{2mu}-1\right]q^{m[(r-1)(s-1)+(s-v)]}$$

if $v=2u+1$.

Proof. Let $\boldsymbol{\tau}_1\in L^s$ be a regular zero of $Q_1(t_1,\dots,t_s)$. By the proof of Lemma 2.1 we have

$$d(r,\boldsymbol{\tau}_1)=d(r-1,\boldsymbol{\tau}_1)q^{m(s-1)}=\dots=q^{(r-1)m(s-1)}.$$

Using (1) we get

$$N_R(r,Q)=[c(1,H)-q^{m(s-v)}]q^{(r-1)m(s-1)}=\left[q^{m(2u-1)}+\nu_{Q_1}(q^{mu}-q^{m(u-1)})-1\right]q^{(r-1)m(s-1)+m(s-v)}$$

when $v=2u$, and

$$N_R(r,Q)=[c(1,H)-q^{m(s-v)}]q^{(r-1)m(s-1)}=\left[q^{2mu}-1\right]q^{(r-1)m(s-1)+m(s-v)}$$

when $v=2u+1$. □

Lemma 2.4. *Let $Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2\in L_r[t_1,\dots,t_s]$ be such that $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2$ in $L[t_1,\dots,t_s]$, with $v<s$. Then $N_S(r,Q)$ is given by*

$$q^{m(s-v)}\left\{q^{\frac{r-2}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\times\frac{q^{(r-2)m(s-1)}-q^{\frac{r-2}{2}m(s-v)}q^{(r-2)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{m(s-1)}q^{2ms}\right\},$$

if r is even, and by

$$q^{m(s-v)}\left\{c(1,Q)q^{\frac{r-3}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\times\frac{q^{(r-3)m(s-1)}-q^{\frac{r-3}{2}m(s-v)}q^{(r-3)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{2m(s-1)}q^{2ms}\right\}$$

if r is odd.

Proof. In this case we have $q^{m(s-v)}$ singular zeroes of Q_1 in L^s. Accordingly to the proof of Lemma 2.2, for each singular zero $\boldsymbol{\tau}_0 \in L^s$ of Q_1, we have

$$\begin{aligned}
d(1,\boldsymbol{\tau}_0)&=1\\
d(2,\boldsymbol{\tau}_0)&=q^{ms}\\
d(3,\boldsymbol{\tau}_0)&=c(1,Q)q^{2ms}\\
d(4,\boldsymbol{\tau}_0)&=c(2,Q)q^{2ms}=\left\{d(2,\boldsymbol{\tau}_0)q^{m(s-v)}+[c(1,Q)-q^{m(s-v)}]q^{m(s-1)}\right\}q^{2ms}\\
&=q^{m(s-v)}q^{3ms}+[c(1,Q)-q^{m(s-v)}]q^{m(s-1)}q^{2ms}\\
d(5,\boldsymbol{\tau}_0)&=c(3,Q)q^{2ms}=\left\{d(3,\boldsymbol{\tau}_0)q^{m(s-v)}+[c(1,Q)-q^{m(s-v)}]q^{2m(s-1)}\right\}q^{2ms}\\
&=c(1,Q)q^{m(s-v)}q^{4ms}+[c(1,Q)-q^{m(s-v)}]q^{2m(s-1)}q^{2ms}\\
d(6,\boldsymbol{\tau}_0)&=q^{2m(s-v)}q^{5ms}+[c(1,Q)-q^{m(s-v)}]\left\{q^{3m(s-1)}q^{2ms}+q^{m(s-1)}q^{m(s-v)}q^{4ms}\right\}\\
d(7,\boldsymbol{\tau}_0)&=c(1,Q)q^{2m(s-v)}q^{6ms}+[c(1,Q)-q^{m(s-v)}]\left\{q^{4m(s-1)}q^{2ms}+q^{2m(s-1)}q^{m(s-v)}q^{4ms}\right\}\\
&\dots
\end{aligned}$$

Therefore,

$$\begin{aligned}
d(r,\boldsymbol{\tau}_0)&=q^{\frac{r-2}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\Big\{q^{(r-3)m(s-1)}q^{2ms}+q^{(r-5)m(s-1)}q^{m(s-v)}q^{4ms}+\dots\\
&\qquad+q^{3m(s-1)}q^{\frac{r-6}{2}m(s-v)}q^{(r-4)ms}+q^{m(s-1)}q^{\frac{r-4}{2}m(s-v)}q^{(r-2)ms}\Big\}\\
&=q^{\frac{r-2}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\left\{\frac{q^{(r-2)m(s-1)}-q^{\frac{r-2}{2}m(s-v)}q^{(r-2)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{m(s-1)}q^{2ms}\right\},
\end{aligned}$$

if r is even, and

$$\begin{aligned}
d(r,\boldsymbol{\tau}_0)&=c(1,Q)q^{\frac{r-3}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\Big\{q^{(r-3)m(s-1)}q^{2ms}+q^{(r-5)m(s-1)}q^{m(s-v)}q^{4ms}+\dots\\
&\qquad+q^{4m(s-1)}q^{\frac{r-7}{2}m(s-v)}q^{(r-5)ms}+q^{2m(s-1)}q^{\frac{r-5}{2}m(s-v)}q^{(r-5)ms}\Big\}\\
&=c(1,Q)q^{\frac{r-3}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)\\
&\qquad-q^{m(s-v)}]\left\{\frac{q^{(r-3)m(s-1)}-q^{\frac{r-3}{2}m(s-v)}q^{(r-3)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{2m(s-1)}q^{2ms}\right\},
\end{aligned}$$

if r is odd. Consequently, $N_S(r,Q)$ equals

$$q^{m(s-v)}\left\{q^{\frac{r-2}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\times\left\{\frac{q^{(r-2)m(s-1)}-q^{\frac{r-2}{2}m(s-v)}q^{(r-2)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{m(s-1)}q^{2ms}\right\}\right\},$$

when r is even, and it equals

$$q^{m(s-v)}\left\{c(1,Q)q^{\frac{r-3}{2}m(s-v)}q^{(r-1)ms}+[c(1,Q)-q^{m(s-v)}]\times\left\{\frac{q^{(r-3)m(s-1)}-q^{\frac{r-3}{2}m(s-v)}q^{(r-3)ms}}{q^{2m(s-1)}-q^{m(s-v)}q^{2ms}}q^{2m(s-1)}q^{2ms}\right\}\right\}$$

when r is odd. □

Proposition 2.3. *Let $Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2$ en $L_r[t_1,\dots,t_s]$ be such that $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2\in L[t_1,\dots,t_s]$, for $v<s$, then the number of zeroes $c(r,Q)$ is given by*

$$c(r,Q)=N_R(r,Q)+N_S(r,Q)\ .$$

Proof. It is inmediate. □

Let us find now the number of solutions of the equation

$$Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2=\beta(z_r), \quad (9)$$

where $\beta(z_r)\in L_r$ is different from zero. In L we have the equation

$$Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2=\beta(z)\ , \quad (10)$$

for $v<s$ and $\beta(z)\neq 0$. If $\beta(z)=0$ we are in the situation of the preceeding proposition. Thus, if $\beta\neq 0$ it is now clear that $(0,\dots,0)$ is not a solution of (10). That means that all the zeroes of (10) are regular. The number of solutions of (10) in L^s accordingly to Proposition 1.1 is

$$\left[q^{m(2u-1)}-\nu_{Q_1}q^{m(u-1)}\right]q^{m(s-v)}$$

if $v=2u$, and

$$\left[q^{2mu}+\omega(\beta(z),\alpha_1,\dots,\alpha_v)q^{mu}\right]q^{m(s-v)}\ ,$$

if $v=2u+1$. Since all of them are regular, the number of descendants of each of these solutions in L_r^s is $q^{m(r-1)(s-1)}$. Therefore, in L_r^s, (9) has

$$\left[q^{m(2u-1)}-\nu_{Q_1}q^{m(u-1)}\right]q^{m(s-v)+m(r-1)(s-1)}$$

if $v=2u$, and

$$\left[q^{2mu}+\omega(\beta(z),\alpha_1,\dots,\alpha_v)q^{mu}\right]q^{m(s-v)+m(r-1)(s-1)}$$

in $v=2u+1$ solutions.

Proposition 2.4. *Let $Q_r(t_1,\dots,t_s)=\alpha_1(z_r)t_1^2+\dots+\alpha_s(z_r)t_s^2$ be a quadratic form in $L_r[t_1,\dots,t_s]$ such that $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_v(z)t_v^2$, with $v<s$. Then the number of solutions of*

$$Q_r(t_1,\dots,t_s)=\beta(z_r),\qquad \beta(z)\neq 0\ ,$$

in L_r^s is given by

$$\left[q^{m(2u-1)}-\nu_{Q_1}q^{m(u-1)}\right]q^{m(s-v)+m(r-1)(s-1)}$$

if $v=2u$, and by

$$\left[q^{2mu}+\omega(\beta(z),\alpha_1,\dots,\alpha_v)q^{mu}\right]q^{m(s-v)+m(r-1)(s-1)}$$

if $v=2u+1$. □

3. Poincaré series

Let $L[[Z]]$ be the algebra of formal power series $\lambda_0+\lambda_1Z+\lambda_2Z^2+\dots$, where $\lambda_j\in L$. Let $H=H(t_1,\dots,t_s)\in L[[Z]][t_1,\dots,t_s]$ and consider the following formal power series

$$P(H,U)=\sum_{j=0}^{\infty}c(j,H)U^j\in\mathbb{Z}[[U]], \quad (11)$$

where $c(0,H)=1$. This series is called the *Poincaré series* of the polynomial H. A conjecture of Borevich & Shafarevich says that (11) is a rational function of U. Our purpose in this section is to compute the Poincaré series of a quadratic form and verify the correctness of this conjecture in this particular case.

Using (1) we obtain for (11) the following expression:

$$\begin{aligned}P(H,U)&=c(0,H)+\sum_{j=1}^{\infty}\sum_{\substack{\tau_1\\ \text{zero of } H_1}}d(j,\tau_1)U^j\\ &=1+\sum_{\substack{\tau_1\\ \text{zero of } H_1}}\sum_{j=1}^{\infty}d(j,\tau_1)U^j\ .\end{aligned}$$

The series $\sum_{j=1}^{\infty}d(j,\tau_1)U^j$ is called the *contribution of the zero* τ_1 to the Poincaré series of H. Thus, if we prove that each one of these contributions is rational function of U, the corresponding Poincaré series will be a rational function. Let us take, thus, the quadratic form

$$Q(t_1,\dots,t_s)=\alpha_1(Z)t_1^2+\dots+\alpha_s(Z)t_s^2$$

en $L[[Z]][t_1,\dots,t_s]$.

Let us define

$$\pi_r(\alpha_j(Z))=\lambda_0+\lambda_1z_r+\dots+\lambda_{r-1}z_r^{r-1}=\alpha_j(z_r)$$

where $\alpha_j(Z)=\lambda_0+\lambda_1Z+\dots+\lambda_kZ^k+\dots$, and z_r is the equivalence class of $p(X)$ modulus $(p(X)^r)$. So $\alpha_j(z_r)$ is the equivalence class of $\alpha_j(Z)$, modulus (Z^r), the ideal generated by Z^r, which in our notation is the equivalence class modulus $(p(X)^r)$. Actually, $L[[Z]]=\operatorname{proj}\lim L_r$ (The details may be found in [**1**, chapter III]). Also, we are able also to compute the number of zeroes $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\dots+\alpha_s(z)t_s^2$, where $\alpha_j(z)$ is the equivalence class modulus $p(X)$ of $\alpha_j(Z)$ (or what amounts to the same thing, $\pi_1(\alpha_j(Z))$).

Let $\tau_1 \in L^s$ be a non singular zero of Q_1 and let $\tau_0 = (0,\ldots,0) \in L^s$ be the unique singular zero of Q_1. Using the results of the foregoing section, we get

$$d(2,\tau_0) = d(2-1,\tau_0)q^{ms} = q^{ms}$$
$$d(r,\tau_0) = c(r-2,Q)q^{2ms} \ ,$$

if $r > 2$. And

$$d(r,\tau_1) = d(r-1,\tau_1)q^{m(s-1)} = \ldots = q^{m(r-1)(s-1)}$$

if $r \geq 1$.

Consequently, the contribution of any non singular zero τ_1 of Q_1 is given by

$$U + q^{m(s-1)}U^2 + q^{2m(s-1)}U^3 + \ldots + q^{(r-1)m(s-1)}U^r + \ldots = \frac{U}{1-q^{m(s-1)}U}.$$

The contribution of τ_0 is

$$U + q^{ms}U^2 + \sum_{r=3}^{\infty} c(r-2,Q)q^{2ms}U^r = U + q^{ms}U^2 + q^{2ms}U^2\sum_{r=3}^{\infty} c(r-2,Q)U^{r-2}$$
$$= U + q^{ms}U^2 + q^{2ms}U^2\sum_{k=1}^{\infty} c(k,Q)U^k = U + q^{ms}U^2 + q^{2ms}U^2\big[P(U,Q)-1\big] \ .$$

In this case

$$P(U,Q) = 1 + \sum_{\tau_1 \text{ zero of } Q_1}\sum_{r=1}^{\infty} d(r,\tau_1) = 1 + \sum_{r=1}^{\infty} d(r,\tau_0) + \sum_{\substack{\tau_1 \text{ regular} \\ \text{zero of } Q_1}}\sum_{r=1}^{\infty} d(r,\tau_1)$$
$$= 1 + U + q^{ms}U^2 + q^{2ms}U^2\big[P(U,Q)-1\big] + \frac{(c(1,Q)-1)U}{1-q^{m(s-1)}U} \ .$$

This last equality implies that

$$\big[P(U,Q)-1\big]\big[1-q^{2ms}U^2\big] = U + q^{ms}U^2 + \frac{(c(1,Q)-1)U}{1-q^{m(s-1)}U} \ ;$$

therefore,

$$P(U,Q) = 1 + \frac{U + q^{ms}U^2 + \frac{(c(1,Q)-1)U}{1-q^{m(s-1)}U}}{1-q^{2ms}U^2} = 1 + \frac{U\Big[(1+q^{ms}U)(1-q^{m(s-1)}U) + c(1,Q) - 1\Big]}{(1-q^{2ms}U^2)(1-q^{m(s-1)}U)}.$$

Using the propositions 1.1 and 1.2 we see that $c(1,Q)$ equals

$$q^{m(2u-1)} + \nu_{Q_1}(q^{mu} - q^{m(u-1)})$$

when $s = 2u$ and it equals q^{2mu} when $s = 2u+1$. We conclude thus that

$$P(U,Q) = 1 + U\Big\{(1+q^{ms}U)(1-q^{m(s-1)}U) + q^{m(2u-1)} + \nu_{Q_1}(q^{mu} - q^{m(u-1)}) - 1\Big\}\frac{1}{(1-q^{2ms}U^2)(1-q^{m(s-1)}U)}$$

if $s = 2u$, and

$$P(U,Q) = 1 + \frac{U\Big[(1+q^{ms}U)(1-q^{m(s-1)}U) + (q^{2mu}-1)\Big]}{(1-q^{2ms}U^2)(1-q^{m(s-1)}U)}$$

if $s = 2u+1$. Using these results we can now verify that the Poincaré series of a diagonal quadratic form Q such that $\operatorname{disc} Q_1 \neq 0$, is a rational function. More precisely,

Proposition 3.1. *Let $Q(t_1,\dots,t_s)=\alpha_1(Z)t_1^2+\ldots+\alpha_s(Z)t_s^2$ be a non singular quadratic form in $L[[Z]][t_1,\dots,t_s]$, such that $\operatorname{disc}Q_1\neq 0$. Then its Poincaré series $P(U,Q)$ is given by*

$$1+U\Big\{(1+q^{ms}U)(1-q^{m(s-1)}U)+q^{m(2u-1)}+\nu_{Q_1}(q^{mu}-q^{m(u-1)})-1\Big\}\frac{1}{(1-q^{2ms}U^2)(1-q^{m(s-1)}U)}$$

when $s=2u$, and by

$$1+\frac{U\Big[(1+q^{ms}U)(1-q^{m(s-1)}U)+(q^{2mu}-1)\Big]}{(1-q^{2ms}U^2)(1-q^{m(s-1)}U)}$$

when $s=2u+1$. □

Next we find the Poincaré series of a quadratic form $Q(t_1,\dots,t_s)\in L[[Z]][t_1,\cdots,T_s]$ for which $\operatorname{disc}Q_1=0$.

Proposition 3.2. *Let $Q(t_1,\dots,t_s)=\alpha_1(Z)t_1^2+\ldots+\alpha_s(Z)t_s^2$ be a quadratic form in $L[[Z]][t_1,\dots,t_s]$, such that $Q_1(t_1,\dots,t_s)=\alpha_1(z)t_1^2+\ldots+\alpha_v(z)t_v^2$, with $v<r$. Then the Poincaré series of Q is given by*

$$1+q^{m(s-v)}U\Big\{(1+q^{ms}U)(1-q^{m(s-1)}U)+q^{m(2u-1)}+\nu_{Q_1}(q^{mu}-q^{m(u-1)})-1\Big\}$$
$$\times\frac{1}{(1-q^{2ms}q^{m(s-v)}U^2)(1-q^{m(s-1)}U)}$$

if $v=2u$, and by

$$1+\frac{q^{m(s-v)}U\Big[(1+q^{ms}U)(1-q^{m(s-1)}U)+(q^{2mu}-1)\Big]}{(1-q^{2ms}q^{m(s-v)}U^2)(1-q^{m(s-1)}U)}$$

if $v=2u+1$.

Proof. Let $\boldsymbol{\tau}_1\in L^s$ be a non singular zero of Q_1 and let $\boldsymbol{\tau}_0\in L^s$ be a singular one. Using the proof of Proposition 3.1 we see that the contribution of any non singular zero $\boldsymbol{\tau}_1$ of Q_1 is

$$U+q^{m(s-1)}U^2+q^{2m(s-1)}U^3+\ldots+q^{(r-1)m(s-1)}U^r+\ldots=\frac{U}{1-q^{m(s-1)}U}.$$

The contribution of each $\boldsymbol{\tau}_0$ is

$$U+q^{ms}U^2+q^{2ms}U^2\big[P(U,Q)-1\big]\,.$$

Then $P(U,Q)$ is given by

$$1+\sum_{\substack{\tau_1\\ \text{zero of }Q_1}}\sum_{r=1}^{\infty}d(r,\boldsymbol{\tau}_1)=1+\sum_{\substack{\tau_0\text{ singular}\\ \text{zero of }Q_1}}\sum_{r=1}^{\infty}d(r,\boldsymbol{\tau}_0)+\sum_{\substack{\tau_1\text{ regular}\\ \text{zero of }Q_1}}\sum_{r=1}^{\infty}d(r,\boldsymbol{\tau}_1)$$
$$=1+\Big[U+q^{ms}U^2\Big]q^{m(s-v)}+q^{2ms}q^{m(s-v)}U^2\big[P(U,Q)-1\big]+\frac{(c(1,Q)-q^{m(s-v)})U}{1-q^{m(s-1)}U}\,.$$

This last equality implies that

$$\big[P(U,Q)-1\big]\big[1-q^{2ms}q^{m(s-v)}U^2\big]=\Big[U+q^{ms}U^2\Big]q^{m(s-v)}+\frac{(c(1,Q)-q^{m(s-v)})U}{1-q^{m(s-1)}U}\;;$$

Therefore, $P(U,Q)$ equals

$$1+\frac{U\Big[(1+q^{ms}U)q^{m(s-v)}(1-q^{m(s-1)}U)+c(1,Q)-q^{m(s-v)}\Big]}{(1-q^{2ms}q^{m(s-v)}U^2)(1-q^{m(s-1)}U)}.$$

We know that

$$c(1,Q)=\Big[q^{m(2u-1)}+\nu_{Q_1}(q^{mu}-q^{m(u-1)})\Big]q^{m(s-v)}$$

when $v = 2u$, and

$$c(1, Q) = q^{2mu} q^{m(s-v)}$$

when $v = 2u + 1$. We conclude that $P(Q, U)$ is equal to

$$1 + q^{m(s-v)} U \Big\{ (1 + q^{ms} U)(1 - q^{m(s-1)} U) + q^{m(2u-1)} + \nu_{Q_1}(q^{mu} - q^{m(u-1)}) - 1 \Big\} \frac{1}{(1 - q^{2ms} q^{m(s-v)} U^2)(1 - q^{m(s-1)} U)}$$

for $v = 2u$, and equals

$$1 + \frac{q^{m(s-v)} U \Big[(1 + q^{ms} U)(1 - q^{m(s-1)} U) + (q^{2mu} - 1) \Big]}{(1 - q^{2ms} q^{m(s-v)} U^2)(1 - q^{m(s-1)} U)}$$

for $v = 2u + 1$. Using these facts we now can verify that the Poincaré series of a diagonal quadratic form Q, with coefficients in $L[[Z]]$ is a rational function. □

References

[1] **Albis, V. S.** *Lecciones sobre la aritmética de polinomios*, policopiado. Departamento de Matemáticas y Estadística, Universidad Nacional de Colombia: Bogotá, 1999.

[2] **Albis, V. S. & Chaparro, R.** *On a conjeture of Borevich and Shafarevich*, Rev. Acad. Colomb. Cienc. **21** (1997), 313–319. [MR: 98g:11130].

[3] **Dickson, L. E.** *Linear Groups with an Exposition of the Galois Field Theory*. Dover Publi.: New York, 1958.