Multiplicative quadratic forms on algebraic varieties

By Akinari HOSHI

Department of Mathematical Sciences, Waseda University, 3-4-1, Ohkubo, Shinjuku-ku, Tokyo 169-8555
(Communicated by Heisuke HIRONAKA, M.I.A., April 14, 2003)

Abstract: In this note we extend Hurwitz-type multiplication of quadratic forms. For a regular quadratic space \((K^n, q)\), we restrict the domain of \(q\) to an algebraic variety \(V \subseteq K^n\) and require a Hurwitz-type “bilinear condition” on \(V\). This means the existence of a bilinear map \(\varphi : K^n \times K^n \to K^n\) such that \(\varphi(V \times V) \subset V\) and \(q(X)q(Y) = q(\varphi(X, Y))\) for any \(X, Y \in V\). We show that the \(m\)-fold Pfister form is multiplicative on certain proper subvariety in \(K^{2m}\) for any \(m\). We also show the existence of multiplicative quadratic forms which are different from Pfister forms on certain algebraic varieties for \(n = 4, 6\). Especially for \(n = 4\) we give a certain family of them.

Key words: Multiplicative quadratic forms; Pfister forms; Dickson’s system.

1. Introduction. Let \(K\) be a field whose characteristic is not 2. In 1898, Hurwitz showed that if there is an identity of the type

\[
(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_2^2) = Z_1^2 + \cdots + Z_n^2,
\]

where the \(Z_k\)’s are bilinear forms of the independent variables \(X_i, Y_j\) over \(K\) then \(n = 1, 2, 4, 8\). In general, for a regular quadratic form \(q(X) := q(X_1, \ldots, X_n)\) over \(K\), \(q(X)\) is called multiplicative if there exists a formula

\[
q(X)q(Y) = q(Z),
\]

where the \(X_i, Y_j\) are independent variables and \(Z_k \in K(X, Y)\). \(q(X)\) is called strictly multiplicative if there exists a formula (1) with \(Z_k\) linear in \(Y_j\) over \(K(X)\). It is known that if \(q(X)\) is isotropic then \(q(X)\) is always multiplicative and in this case \(q(X)\) is strictly multiplicative if and only if \(q(X)\) is hyperbolic (see [4] or [7]). A quadratic form is called Pfister form if it is expressible as a tensor product of binary quadratic forms of the type \((1, a)\). We denote by \(\langle a_1, a_2, \ldots, a_m \rangle\) the \(m\)-fold Pfister form \((1, a_1) \otimes (1, a_2) \otimes \cdots \otimes (1, a_m)\). In 1965, A. Pfister showed the following theorem.

Theorem (Pfister [3]). If \(q\) is a Pfister form, then \(q\) is strictly multiplicative. Conversely if \(q\) is an anisotropic multiplicative form over \(K\), then \(q\) must be a Pfister form.

Let \(D_K(n)\) be the set of values in \(K^n\) represented by a sum of \(n\) squares in \(K\), namely

\[D_K(n) = \{ \alpha \in K^n \mid \alpha = \alpha_1^2 + \cdots + \alpha_n^2, \ \alpha_j \in K \}.\]

The Stufe (or level) of a field \(K\) is defined as \(s(K) := \text{Inf}(n \in \mathbb{N} : -1 \in D_K(n))\). From above theorem, we see that if \(n\) is a power of 2 then \(D_K(n)\) is a multiplicative group. Using this fact, Pfister proved the following remarkable theorem (see [2] or [7]).

Theorem (Pfister). For any field \(K\), \(s(K)\) is, if finite, always a power of 2. Conversely every power of 2 is the Stufe of some field \(K\).

2. Multiplicative quadratic forms on algebraic varieties. In this section, we extend the Hurwitz-type multiplicative quadratic forms in different way. For a regular quadratic space \((K^n, q)\), we restrict the domain of \(q\) to an algebraic variety \(V \subseteq K^n\). Furthermore we require the Hurwitz-type “bilinear condition” for \(q\) on \(V\). More precisely, we make the following.

Definition. Let \(V \subseteq K^n\) be an algebraic variety. We say a regular quadratic form \(q(X)\) is multiplicative on \(V\) if there is a bilinear map \(\varphi : K^n \times K^n \to K^n\) such that

\[
\varphi(V \times V) \subset V \quad \text{and} \quad q(X)q(Y) = q(\varphi(X, Y)) \quad \text{for any} \quad X, Y \in V.
\]

Then the following natural problems arise.

Problem 1. Given a regular quadratic form \(q(X)\), determine whether an algebraic variety \(V \subseteq K^n\) exists on which \(q(X)\) is multiplicative.

Problem 2. Given an algebraic variety \(V \subseteq K^n\), determine whether a quadratic form \(q(X)\) which is multiplicative on \(V\) exists.
Problem 3. If Problem 1 or 2 is affirmative, find a bilinear map \( \varphi \) explicitly.

Note that in the classical case \( V = K^n \), an anisotropic quadratic form is multiplicative if and only if it is a Pfister form. Moreover, when we require the Hurwitz-type “bilinear condition” a multiplicative quadratic form exists only for dimension 1, 2, 4 and 8. In this note we assume that the quadratic form is diagonal in order to simplify an argument.

We first describe a simple example which is a slight generalization of Hurwitz’s theorem (see [5]). Let \( A \) be a finite-dimensional \( K \)-algebra with involution \( \tau \). We define an algebraic variety \( V_\tau := \{ x \in A \mid x \cdot x^\tau \in K \} \) and a quadratic form \( N_\tau(\alpha) := \alpha \cdot \alpha^\tau \), \( \alpha \in V_\tau \). Then we see that

\[
N_\tau(\alpha\beta) = \tau(\alpha\beta)^\tau = \alpha\beta^\tau \alpha^\tau = N_\tau(\alpha)N_\tau(\beta), \quad \text{for any} \quad \alpha, \beta \in V_\tau.
\]

In particular we consider the following case, from which one can recover the Pfister form in a natural way. Let \( a_1, \ldots, a_m \in K^\times \) and suppose \( L = K(\sqrt{-a_1}, \ldots, \sqrt{-a_m}) \) is an extension field of degree \( 2^m \) over \( K \). We put \( S_m := \{ 1, 2, \ldots, m \} \) then \( (e_j := \prod_{i \neq j} \sqrt{-a_i} \mid J \subseteq S_m \) is a basis for \( L/K \). For \( 1 \leq i \leq m \), we define \( \sigma_i \in \text{Aut}(L/K) \) by

\[
\sigma_i(\sqrt{-a_k}) = \begin{cases} \sqrt{-a_k} & \text{if } k = i, \\ -\sqrt{-a_k} & \text{if } k \neq i. \end{cases}
\]

Hence \( \text{Gal}(L/K) \cong \langle \sigma_1, \ldots, \sigma_m \rangle \). We now consider \( \tau \in \text{Gal}(L/K) \) of order 2 and define \( \text{sgn}_\tau(i) \in \{ \pm 1 \} \) for \( 1 \leq i \leq m \) by the equation

\[
\tau(\sqrt{-a_i}) = \text{sgn}_\tau(i)\sqrt{-a_i}.
\]

For \( \alpha \in L \), we write

\[
\alpha = \sum_{I \subseteq S_m} u_I e_I, \quad u_I \in K
\]

and define

\[
N_\tau(\alpha) := N_{L/L(\tau)}(\alpha) = \alpha \cdot \alpha^\tau \in L(\tau).
\]

Then there are \( 2^{m-1} \) quadratic forms \( f_j(X) := f_j(X_1, \ldots, X_{2^m}) \), \( (J \subseteq S_m, \tau(e_j) = e_j) \) such that

\[
N_\tau(\alpha) = \sum_{J \subseteq S_m, \tau(e_j) = e_j} f_J(u_J) e_J.
\]

Note that \( f_0(X) = |I_a| \) is the \( m \)-fold Pfister form \( \langle |I_a| a_1, \ldots, |I_a| a_m \rangle \). We see that

\[
\{ \alpha \in L^\times \mid N_\tau(\alpha) \in K \}
\]

is a multiplicative group. Therefore we obtain the following fundamental proposition of the theory of multiplicative quadratic forms on algebraic varieties.

**Proposition 1.** Let \( f_j(X) \) be \( 2^{m-1} \) quadratic forms defined in (2) and let \( V \) be defined by the \( 2^{m-1} - 1 \) equations \( f_j(X) = 0 \), \( (J \neq \emptyset) \). The \( m \)-fold Pfister form \( f_0(X) = \langle \langle -\text{sgn}_\tau(1) a_1, \ldots, -\text{sgn}_\tau(m) a_m \rangle \rangle \) is multiplicative on \( V \).

Let \( V \subseteq K^m \) be an algebraic variety and \( q \) be a quadratic form on \( V \). Define \( D_V(q) \) to be the set of values in \( K^\times \) represented by \( q \) on \( V \), namely

\[
D_V(q) = \{ \alpha \in K^\times \mid \alpha = q(\alpha_1, \ldots, \alpha_n), \quad \text{for} \quad (\alpha_1, \ldots, \alpha_n) \in V \}.
\]

We see that if \( q \) is multiplicative on \( V \) and represents 1 then \( D_V(q) \) is a multiplicative group. Note that we can also consider \( q \) over a commutative ring \( R \) requiring the Hurwitz-type “bilinear condition” over \( R \). We shall give an application which is the case over the ring of integers \( \mathbf{Z} \) in Section 3.

We now present an example of Proposition 1.

**Example 2.** The case \( m = 2 \). Suppose \( L = K(\sqrt{-a_1}, \sqrt{-a_2}) \) is a biquadratic extension field of \( K \) and let \( \tau \in \text{Gal}(L/K) \) of order 2 such that

\[
\tau(\sqrt{-a_1}) = -\sqrt{-a_1}, \quad \tau(\sqrt{-a_2}) = -\sqrt{-a_2}.
\]

For \( \alpha, \beta \in L \), we write

\[
\alpha = X_1 + X_2\sqrt{-a_1} + X_3\sqrt{-a_2} + X_4\sqrt{-a_1}\sqrt{-a_2},
\]

\[
\beta = Y_1 + Y_2\sqrt{-a_1} + Y_3\sqrt{-a_2} + Y_4\sqrt{-a_1}\sqrt{-a_2}.
\]

We have

\[
N_\tau(\alpha) = X_1^2 + a_1X_2^2 + a_2X_3^2 + a_1a_2X_4^2
\]

\[
+ 2(X_1X_4 - X_2X_3)\sqrt{-a_1}\sqrt{-a_2}
\]

and put

\[
q(X) := f_0(X) = X_1^2 + a_1X_2^2 + a_2X_3^2 + a_1a_2X_4^2,
\]

\[
h(X) := f_1(X) = 2(X_1X_4 - X_2X_3).
\]

From Proposition 1, \( q(X) \) is multiplicative on \( V \):

\[
h(X) = 0. \quad \text{Namely if} \quad h(X) = 0 \quad \text{then there is the bilinear map} \quad \varphi : K^4 \times K^4 \to K^4 \quad \text{such that} \quad q(X)q(Y) = q(\varphi(X, Y)) \quad \text{and} \quad h(\varphi(X, Y)) = 0.
\]

Since \( N_\tau(\alpha)N_\tau(\beta) = N_\tau(\alpha\beta) \) and

\[
\alpha\beta = (X_1Y_1 - a_1X_2Y_2 - a_2X_3Y_3 + a_1a_2X_4Y_4)
\]

\[
+ (X_2Y_1 + X_1Y_2 - a_2X_3Y_3 - a_1X_2Y_4)\sqrt{-a_1}
\]

\[
+ (X_3Y_1 - a_1X_2Y_3 + X_2Y_1 - a_1X_3Y_4)\sqrt{-a_2}
\]

\[
+ (X_4Y_1 + X_3Y_2 + X_2Y_3 + X_1Y_4)\sqrt{-a_1}\sqrt{-a_2},
\]

\[
\langle \langle -\text{sgn}_\tau(1) a_1, \ldots, -\text{sgn}_\tau(m) a_m \rangle \rangle.
\]

We see that
where the X 2 No. 4] Multiplicative quadratic forms on algebraic varieties 73

the following equations.

Problem 4. Does there exist a quadratic form The following problem arises as the next natural question after Proposition 1.

Remark. For Corollary 3, the 2-fold Pfister form q(X) = X 2 + a1X 2 + a2X 3 + a1a2X 4, a1, a2 ∈ K x is multiplicative on V : h(X) = 0 without the supposition that K(√−a1, √−a2) is a field of degree 4 over K as in Example 2.

The following problem arises as the next natural question after Proposition 1.

Problem 4. Does there exist a quadratic form q(X) which is different from a Pfister form and multiplicative on an algebraic variety K x ?

for any λ ∈ K x , q(X) = X 2 + (b^2 + 4acαλ^2X 2 + (b^2 + 4ac)αX 3 + (b^2 + 4ac)αλ^2X 4) is multiplicative on V(a,b,c). Moreover the bilinear map ϕ is given explicitly as follows:

ϕ(X, Y) = 
(X 1Y 1 + (b^2 + 4ac)αλ^2X 2Y 2 
+ (b^2 + 4ac)αλX 3Y 3 + (b^2 + 4ac)αλX 4Y 4, 
X 2Y 1 + X 1Y 2 + 2bX 3Y 3 + bX 4Y 4 
+ bX 3Y 3 + bX 4Y 4 - 2eX 4Y 4, 
X 3Y 1 + 2acλX 3Y 2 + 2acλX 4Y 2 
- X 1Y 2 - 2acλX 2Y 3 - 2acλX 2Y 4, 
X 4Y 1 + abλX 2Y 2 - 2acλX 2Y 4 
- abλX 2Y 3 - X 1Y 4 + 2acλX 2Y 4).

Proof. Put f(X) := X 1X 2 + aX 3X 2 + bX 3X 4 - cX 2. Using ϕ, we can show the following relations by direct calculation.

\[ q(X)q(Y) = q(\varphi(X, Y)) \]
\[ - 4(b^2 + 4ac)\alpha\lambda^2f(X)f(Y), \]
\[ f(\varphi(X, Y)) = f(X)f(Y) + f(\varphi(Y, X)). \]

Corollary 5. Let a, b, c, V(a,b,c) be as above in Theorem 4. Suppose \( b^2 + 4ac \notin K^{x^2} \). Then there are infinitely many 4-dimensional diagonal multiplicative quadratic forms on V(a,b,c) which are different from Pfister forms.

Remark. For Theorem 4, if we consider q(X) over the field K(√b^2 + 4ac) then we see that Theorem 4 is a consequence of Proposition 1. In fact if we use the non-singular linear transformation of variables as follows:

\[ X_1 \rightarrow \tilde{X}_1, \quad X_2 \rightarrow \tilde{X}_4, \]
\[ X_3 \rightarrow \frac{1}{2a} \left( \tilde{X}_2 - a\tilde{X}_3 - b(\tilde{X}_2 + a\tilde{X}_3) \right), \]
\[ X_4 \rightarrow \frac{\tilde{X}_2 + a\tilde{X}_3}{\sqrt{b^2 + 4ac}}, \]

then we can show that q(\tilde{X}) and f(\tilde{X}) in Theorem 4 are transformed to

\[ q(\tilde{X}) = \tilde{X}_1^2 + m_1\tilde{X}_2^2 + m_2\tilde{X}_3^2 + m_3\tilde{X}_4^2, \]
\[ f(\tilde{X}) = \tilde{X}_1\tilde{X}_4 - \tilde{X}_2\tilde{X}_3, \]

where

\[ m_1 = \frac{\lambda}{2a} \left( b^2 + 4ac - b\sqrt{b^2 + 4ac} \right), \]
\[ m_2 = \frac{a\lambda}{2} \left( b^2 + 4ac + b\sqrt{b^2 + 4ac} \right), \]
\[ m_3 = m_1m_2 = (b^2 + 4ac)\alpha\lambda^2. \]

The following theorem shows that, in contrast to the classical case, a multiplicative quadratic form q(X) exists in the non-2-power dimensional case for some algebraic varieties V.

Theorem 6. Let q(X) = X 1^2 + 21X 2^2 + 21X 3^2 + 21X 4^2 + 14X 5^2 + 42X 6^2 and V:

\[ \begin{cases} 
3X 2^2 + 6X 2X 3 - 6X 2X 4 + 12X 5X 4 \\
-3X 2^2 + 3X 3^2 + 4X 1X 6 + 2X 5X 6 - 9X 6^2 = 0, \\
12X 2X 3 + 3X 3^2 + 6X 2X 4 + 6X 3X 4 - 3X 4^2 \\
+ 2X 1X 5 + X 5^2 + 2X 1X 6 + 10X 5X 6 - 3X 6^2 = 0.
\end{cases} \]
Then $q(X)$ is multiplicative on $V$. Moreover the bilinear map $\varphi$ is given explicitly as follows:

\[ \varphi(X, Y) = \]
\[ (-X_1Y_1 - 21X_2Y_2 - 21X_3Y_3 - 14X_3Y_5 - 42X_6Y_6, \]
\[ X_2Y_1 - X_1Y_2 + X_3Y_2 - 3X_6Y_2 - 3X_5Y_3 - 3X_5Y_4 + 3X_6Y_4 - X_2Y_5 + 3X_3Y_5 + 3X_4Y_5 + 3X_2Y_6 + 3X_3Y_6 - 3X_4Y_6, \]
\[ X_3Y_1 - 3X_5Y_2 - 3X_6Y_2 - X_1Y_3 - 2X_2Y_3 - 6X_6Y_4 + 3X_2Y_5 + 3X_2Y_6 + 6X_4Y_6, \]
\[ X_4Y_1 - 3X_5Y_2 + 3X_6Y_2 - 6X_6Y_3 - X_1Y_4 + X_3Y_4 + 3X_6Y_4 + 3X_3Y_5 - 3X_2Y_6 + 6X_3Y_6 - 3X_4Y_6, \]
\[ (-2X_3Y_1 + 3X_2Y_2 - 9X_3Y_2 - 9X_1Y_3 - 6X_2Y_3 - 9X_2Y_4 + 3X_4Y_4 - 2X_1Y_5 + X_3Y_5 - 9X_6Y_5 - 9X_5Y_6)/2, \]
\[ (-2X_6Y_1 - 3X_2Y_2 - 3X_3Y_2 + 3X_4Y_2 - 3X_2Y_3 - 3X_6Y_6 - 6X_4Y_3 + 3X_2Y_4 - 6X_3Y_4 + 3X_4Y_4 - 3X_5Y_5 - X_6Y_5 - 2X_1Y_6 - X_5Y_6 + 9X_6Y_6)/2. \]

**Proof.** We put

\[ f_1(X) := 3X_2^2 + 6X_2X_3 - 6X_2X_4 + 12X_3X_4 - 3X_4^2 + 3X_3^2 + 4X_1X_6 + 2X_3X_6 - 9X_6^2, \]
\[ f_2(X) := 12X_2X_3 + 3X_2^2 + 6X_2X_4 + 6X_3X_4 - 3X_4^2 + 2X_1X_5 + X_2^2 + 2X_1X_6 + 10X_3X_6 - 3X_6^2. \]

Using $\varphi$, we find the following relations which can be checked by direct calculation.

\[ q(X)q(Y) = q(\varphi(X, Y)) - 14f_1(X)f_1(Y) + 7f_1(X)f_2(Y) + 7f_2(X)f_1(Y) - 14f_2(X)f_2(Y), \]
\[ f_1(\varphi(X, Y)) = q(X)f_1(Y) + f_1(X)q(Y) - 2f_1(X)f_1(Y) - f_1(X)f_2(Y) - f_2(X)f_1(Y) + 3f_2(X)f_2(Y), \]
\[ f_2(\varphi(X, Y)) = q(X)f_2(Y) + f_2(X)q(Y) - 3f_1(X)f_1(Y) + 2f_1(X)f_2(Y) + 2f_2(X)f_1(Y) + f_2(X)f_2(Y). \]

**3. Applications.** We give one example of applications which use the multiplicative quadratic forms on algebraic varieties over the ring of integers $\mathbb{Z}$.

Let $p$ be a prime $\equiv 1 \pmod{5}$. It is well known that the following system of diophantine equations has exactly four integer solutions.

\begin{align*}
(3) & \quad 16p = x^2 + 125uv^2 + 50v^2 + 50u^2, \\
(4) & \quad xw = uv^2 - 4uv - u^2, \\
(5) & \quad x \equiv -1 \pmod{5}.
\end{align*}

This system is often called “Dickson’s system” since above result was discovered by Dickson [1] in 1935. If $(x, w, v, u)$ is one integer solution then the remaining three are $(x, -w, -u, v)$, $(x, w, -v, u)$, $(x, -w, u, -v)$.

We are able to apply Theorem 4 to above system of diophantine equations. Using Theorem 4 for $a = -1$, $b = 4$, $c = -1$, $\lambda = -5/2$, we see that the quadratic form $q(X) = X_1^2 + 125X_2^2 + 50X_3^2 + 50X_4^2$ is multiplicative on $V : X_1X_2 = X_3^2 - 4X_3X_4 - X_4^2$. The bilinear map $\varphi : \mathbb{Z}^4 \times \mathbb{Z}^4 \rightarrow \mathbb{Z}^4$ such that $q(X)q(Y) = q(\varphi(X, Y))$ is given as follows:

\[ \varphi(X, Y) = \]
\[ (X_1Y_1 + 125X_2Y_2 + 50X_3Y_3 + 50X_4Y_4, \]
\[ X_2Y_1 + X_1Y_2 - 2X_2Y_3 + X_4Y_3 - 4X_4Y_4 + 4X_3Y_4 + 2X_4Y_4 + 10X_3X_6 - 10X_2Y_3 - X_1Y_3 - X_2Y_3 - 10X_3Y_3, \]
\[ X_4Y_1 + 10X_3Y_2 + 5X_2Y_2 - 10X_2X_6 - 5X_2Y_4). \]

Using this $\varphi$, we obtain the following extended result of Dickson’s system.

**Theorem 7.** Let $N$ be an integer such that $N = p_1^{t_1}p_2^{t_2} \cdots p_k^{t_k}$, where $p_i \equiv 1 \pmod{5}$ is a prime for each $i$. Then the system of diophantine equations

\[ (3) - (5) \text{ with } N \text{ instead of } p \text{ has integer solutions.} \]

Let $p_1$ and $p_2$ be primes such that $p_1 \equiv p_2 \equiv 1 \pmod{5}$. Let $(x_{p_1}, w_{p_1}, v_{p_1}, u_{p_1})$ (resp. $(x_{p_2}, w_{p_2}, v_{p_2}, u_{p_2})$) be one of integer solutions of the system of (3)–(5) which belongs to $p_1$ (resp. $p_2$). For the product $p_1p_2$, we define $(x_{p_1p_2}, w_{p_1p_2}, v_{p_1p_2}, u_{p_1p_2}) \in \mathbb{Z}[1/2]^4$ by

\[ (x_{p_1p_2}, w_{p_1p_2}, v_{p_1p_2}, u_{p_1p_2}) := \varphi((x_{p_1}, w_{p_1}, v_{p_1}, u_{p_1}), (x_{p_2}, w_{p_2}, v_{p_2}, u_{p_2}))/4, \]

where $\varphi$ is the bilinear map in (6). Furthermore,
we define \((x_N, w_N, v_N, u_N) \in \mathbb{Z}[1/2]^4\), for \(N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\), each \(p_i\) is prime \(\equiv 1 \pmod{5}\), by repeating and using the definition (7). We see that the 4-tuple \((x_N, w_N, v_N, u_N)\) is the solution of the Dickson’s system (3)–(5) which belongs to \(N\). Therefore to prove Theorem 7 we have to show that the 4-tuple is integral: \((x_N, w_N, v_N, u_N) \in \mathbb{Z}^4\).

Lemma 8. Let \(p\) be a prime \(\equiv 1 \pmod{5}\). Then the solution \((x_p, w_p, v_p, u_p) \in \mathbb{Z}^4\) of the system (3)–(5) satisfies the following congruences.

\[
\begin{align*}
-x_p + w_p + 2u_p & \equiv 0 \pmod{4}, \\
-x_p - w_p + 2v_p & \equiv 0 \pmod{4}.
\end{align*}
\]

Proof. See, for example, [6, Lemma 1(d)].

Lemma 9. Let \(N_1 = l_1^{a_1} l_2^{a_2} \cdots l_m^{a_m}\) and \(N_2 = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}\), each \(q_k\) is prime \(\equiv 1 \pmod{5}\). If \((x_{N_1}, w_{N_1}, v_{N_1}, u_{N_1}) \in \mathbb{Z}^4\) and it satisfies (8) for \(i = 1, 2\) then \((x_{N_1 N_2}, w_{N_1 N_2}, v_{N_1 N_2}, u_{N_1 N_2}) \in \mathbb{Z}^4\) and it also satisfies (8).

Proof. If \((x_{N_1}, w_{N_1}, v_{N_1}, u_{N_1}) \in \mathbb{Z}^4\) and it satisfies (8) for \(i = 1, 2\) then there are \(s_1, t_1, s_2, t_2 \in \mathbb{Z}\) such that

\[
\begin{align*}
x_{N_i} &= w_{N_i} + 2u_{N_i} + 4s_i, \quad (i = 1, 2), \\
v_{N_i} &= w_{N_i} + u_{N_i} + 2t_i, \quad (i = 1, 2).
\end{align*}
\]

By the definition (7) and using (9) we see that the 4-tuple \((x_{N_1 N_2}, w_{N_1 N_2}, v_{N_1 N_2}, u_{N_1 N_2})\) is equal to

\[
\begin{align*}
4s_1 s_2 + 50t_1 t_2 + 2s_2 u_1 + 25t_2 u_1 + 2s_1 u_2 + 25t_1 u_2 + 6u_1 u_2 + s_2 w_1 + 25t_2 w_1 + 13u_2 w_1 + s_1 w_2 + 25t_1 w_2 + 13u_1 w_2 + 44w_1 w_2, \\
s_2 w_1 - 2t_1 t_2 + t_2 u_1 + t_1 u_2 \\
+ 2u_1 u_2 - t_2 w_1 + u_2 w_1 - s_1 w_2 - t_1 w_2 + u_1 w_2, \\
2s_1 t_1 - 2s_1 t_2 + 2s_2 u_1 - t_2 u_1 - s_1 u_2 + t_1 u_2 \\
+ s_2 w_1 + 2t_2 w_1 - u_2 w_1 - s_1 w_2 - 2t_1 w_2 + u_1 w_2, \\
s_2 u_1 - s_1 u_2 - 5t_2 w_1 - 4u_2 w_1 + 5t_1 w_2 + 4u_1 w_2),
\end{align*}
\]

where \((u_i, v_i) = (w_N, u_N)\) for \(i = 1, 2\). Hence \((x_{N_1 N_2}, w_{N_1 N_2}, v_{N_1 N_2}, u_{N_1 N_2}) \in \mathbb{Z}^4\). Using this it is easily verified that this 4-tuple satisfies (8).

Proof of Theorem 7. By the definition (7), the system of diophantine equations (3)–(4) which belongs to \(N\) has solutions \((x_N, w_N, v_N, u_N) \in \mathbb{Z}[1/2]^4\). By Lemma 8 and Lemma 9, we obtain that this 4-tuple \((x_N, w_N, v_N, u_N)\) is in \(\mathbb{Z}^4\). It remains to show that \(x_N \equiv -1 \pmod{5}\). This follows from (6) and (7).

It is well known that the Dickson’s system (3)–(5) is related very deeply to the Jacobi sums. In fact for a prime \(p \equiv 1 \pmod{5}\) the solution of Dickson’s system (3)–(5) give the coefficients of Jacobi sum for \(F_p\). We can study the Jacobi sum for \(F_q, q = p^n\) in detail by using Theorem 4. We shall discuss it in separate paper because it is much more elaborate.

Acknowledgement. The author thanks Professor K. Hashimoto who gave him various suggestions during this study.

References