Adv. Geom. **4** (2004), 241–261

Advances in Geometry

Association schemes of affine type over finite rings

Hajime Tanaka*

(Communicated by E. Bannai)

Abstract. Kwok [10] studied the association schemes obtained by the action of the semidirect products of the orthogonal groups over the finite fields and the underlying vector spaces. They are called the assiciation schemes of affine type. In this paper, we define the association schemes of affine type over the finite ring $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ where q is a prime power in the same manner, and calculate their character tables explicitly, using the method in Medrano et al. [13] and DeDeo [8]. In particular, it turns out that the character tables are described in terms of the Kloosterman sums. We also show that these association schemes are self-dual.

Introduction

The purpose of the present paper is to study a certain kind of association schemes related to the orthogonal groups over the finite ring $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, where $q = p^r$ is a prime power.

Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a non-degenerate quadratic form over the finite field $\mathbb{F}_q$ and $O(\mathbb{F}_q^n, f)$ its orthogonal group. Since $-\mathrm{id}$ is contained in $O(\mathbb{F}_q^n, f)$, the action of the semidirect product $O(\mathbb{F}_q^n, f) \ltimes \mathbb{F}_q^n$ on $\mathbb{F}_q^n$ defines a symmetric association scheme $\mathfrak{X}(O(\mathbb{F}_q^n, f), \mathbb{F}_q^n)$. Kwok [10] called this association scheme an association scheme of affine type, and calculated its character table completely (see also [12], [5]).

We define the association schemes of affine type over the finite rings $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$ ($k \in \mathbb{N}$) in the same manner. However, by the Chinese remainder theorem, it is enough to consider the case where k is a prime power ([1, p. 59]). It seems that these association schemes had not been studied, but some related results can be found in Medrano et al. [13] and DeDeo [8]. Namely, in [13], [8], the finite Euclidean graph $X_q(n, a)$ over $\mathbb{Z}_q$ with $a \in \mathbb{Z}_q^\times = \mathbb{Z}_q \backslash p\mathbb{Z}_q$ is defined as the graph with the vertex set $\mathbb{Z}_q^n$, and the edge set

$$E = \{(x, y) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n \mid d(x, y) = a\},$$

*The author is supported in part by a grant from the Japan Society for the Promotion of Science.

where $d(x, y) \in \mathbb{Z}_q$ is the "distance" defined by

$$d(x, y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2.$$

We will show that if q is an odd prime power, then in our language these graphs are part of the relations of $\mathfrak{X}(O(\mathbb{Z}_q^n, d(\cdot, 0)), \mathbb{Z}_q^n)$, the association scheme of affine type with respect to the non-degenerate quadratic form $d(x, 0) = x_1^2 + x_2^2 + \cdots + x_n^2$ ($d(\cdot, 0)$ is degenerate if q is even).

In this paper, we determine the character table of the symmetric association scheme $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$ explicitly for all non-degenerate quadratic forms on $\mathbb{Z}_q^n$ (for both odd q and even q). These results are given in Theorem 2.10, Theorem 2.12 and Theorem 2.15. In particular, we will be able to see a phenomenon similar to the Ennola type dualities observed in [4]. Also, as an immediate consequence of these calculations, we verify that these association schemes are self-dual.

The outline of the paper is as follows. In Section 1, we review some basic notions on commutative association schemes, and classify the non-degenerate quadratic forms on $\mathbb{Z}_q^n$ completely. In Section 2, the character tables are calculated explicitly. The discussion in this section is almost parallel to those in [13], [8]. We will find that the method of computing the eigenvalues of the graphs $X_q(n, a)$ used successfully in [13], [8] also works in our case. (It seems possible to obtain the results in [10], by the method in [12], [13], [8].) In particular, the character tables are described in terms of the Kloosterman sums over $\mathbb{Z}_q$.

Acknowledgement. The author would like to thank Mr. Makoto Tagami for some useful discussions.

1 Preliminaries and the classification of the non-degenerate quadratic forms over $\mathbb{Z}_q$

1.1 Preliminaries on commutative association schemes. Here, we recall some basic notions on commutative association schemes. We refer the reader to [3], [7], [2] for the background in the theory of these objects.

Let $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ be a commutative association scheme with the adjacency matrices $A_0 = I, A_1, \ldots, A_d$, where I is the identity matrix of degree $|x|$. The algebra $\mathfrak{A}$ of dimension $d + 1$, generated by $A_0, \ldots, A_d$ over the complex number field $\mathbb{C}$, is called the Bose–Mesner algebra of $\mathfrak{X}$. If we consider the action of $\mathfrak{A}$ on the vector space $V = \mathbb{C}^{|X|}$ indexed by the elements of X, then V is decomposed into the direct sum of the maximal common eigenspaces:

$$V = V_0 \perp V_1 \perp \cdots \perp V_d,$$

where V_0 is the one-dimensional subspace spanned by the all-one vector. Let $E_i : V \to V_i$ be the orthogonal projection ($0 \leqslant i \leqslant d$). Then the set $\{E_0, E_1, \ldots, E_d\}$ forms another basis of $\mathfrak{A}$, and the base change matrix $P = (p_i(j))$ is called the *character table* or the *first eigenmatrix* of $\mathfrak{X}$:

$$A_i = \sum_{j=0}^{d} p_i(j) E_j \quad (0 \leqslant i \leqslant d)$$

(the (j,i)-entry of P is $p_i(j)$). In particular, $k_i = p_i(0)$ is the valency of the regular graph (X, R_i). The *second eigenmatrix* $Q = (q_i(j))$ of $\mathfrak{X}$ is defined by $Q = |X|P^{-1}$, that is,

$$|X|E_i = \sum_{j=0}^{d} q_i(j) A_j \quad (0 \leqslant i \leqslant d).$$

The numbers $m_i = q_i(0) = \dim V_i$ $(0 \leqslant i \leqslant d)$ are called the multiplicities of $\mathfrak{X}$. Notice that the first eigenmatrix P, together with the multiplicities of $\mathfrak{X}$, gives complete information of the spectra of the graphs (X, R_i) $(1 \leqslant i \leqslant d)$.

Now, assume that $\mathfrak{X}$ is symmetric and that the underlying set X has the structure of an abelian group. We call $\mathfrak{X}$ a *translation association scheme* if for $0 \leqslant i \leqslant d$ and $z \in X$ we have

$$(x, y) \in R_i \Rightarrow (x + z, y + z) \in R_i.$$

For such an association scheme, there is a natural way to define the *dual scheme* $\mathfrak{X}^* = (X^*, \{R_i^*\}_{0 \leqslant i \leqslant d})$, where X^* denotes the character group of X. Namely, we define the relation R_i^* by

$$(\mu, v) \in R_i^* \Leftrightarrow v\mu^{-1} \in V_i$$

(considered as a vector of V). Then, $\mathfrak{X}^* = (X^*, \{R_i^*\}_{0 \leqslant i \leqslant d})$ becomes a translation association scheme with the eigenmatrices $P^* = Q$ and $Q^* = P$ (see e.g. [7, §2.10B] or [3, §2.6]). The translation association scheme $\mathfrak{X}$ is called *self-dual* if it is isomorphic to its dual $\mathfrak{X}^*$. In particular, if $\mathfrak{X}$ is self-dual, then clearly we have $P = Q$.

1.2 The classification of the non-degenerate quadratic forms over $\mathbb{Z}_q$. Let $q = p^r$ with p prime. If a is a unit in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, we denote its multiplicative inverse in $\mathbb{Z}_q$ by $a^{[-1]}$. Sometimes we identify the ring $\mathbb{Z}_q$ with the set $\{0, 1, \ldots, q-1\}$, and regard $\mathbb{Z}_{p^l}^n$ $(l < r)$ as a subset of $\mathbb{Z}_q^n$.

For a nonzero element a of $\mathbb{Z}_q$, we denote the largest integer l such that p^l divides a by $\mathrm{ord}_p^{(r)}(a)$. Conventionally, $\mathrm{ord}_p^{(r)}(0)$ is defined to be r. Also, if $x = (x_1, x_2, \ldots, x_n)$ is an element of $\mathbb{Z}_q^n$, then we define $\mathrm{ord}_p^{(r)}(x)$ by

$$\mathrm{ord}_p^{(r)}(x) = \min_{1 \leqslant i \leqslant n} \mathrm{ord}_p^{(r)}(x_i).$$

The reduction of x modulo $p\mathbb{Z}_q^n$ is denoted by $\bar{x} \in \mathbb{Z}_p^n$. If $\mathrm{ord}_p^{(r)}(x) > 0$, then there exists a unique element y of $\mathbb{Z}_{p^{r-1}}^n$ such that $x = py$, and we write $y = \frac{1}{p}x$.

For later use, we prove the following lemma.

Lemma 1.1. *Let W be a submodule of $\mathbb{Z}_q^n$. Then W is a direct summand of $\mathbb{Z}_q^n$ if and only if it is free.*

Proof. First, suppose that W is a direct summand of $\mathbb{Z}_q^n$ so that W is projective. Then since $\mathbb{Z}_q$ is local with the maximal ideal $p\mathbb{Z}_q$, W is free (see e.g. [11, p. 9, Theorem 2.5]).

Conversely, suppose that W is free. Let $\{f_1, f_2, \dots, f_k\}$ be a basis of W. Then it follows that $\bar{f}_1, \bar{f}_2, \dots, \bar{f}_k \in \mathbb{Z}_p^n$ are linearly independent over $\mathbb{Z}_p$. In fact, assume that $\bar{a}_1\bar{f}_1 + \bar{a}_2\bar{f}_2 + \cdots + \bar{a}_k\bar{f}_k = \bar{0}$ holds for some $a_1, a_2, \dots, a_k \in \mathbb{Z}_q$. Then we have

$$f = \sum_{p \nmid a_i} a_i f_i \in p\mathbb{Z}_q^n.$$

This implies $f = 0$, since otherwise $p^{r-1}f$ does not vanish, which is a contradiction. Thus, we have $\bar{a}_i = \bar{0}$ for all i, as desired. Now, take $f_{k+1}, \dots, f_n \in \mathbb{Z}_q^n$ so that $\{\bar{f}_1, \bar{f}_2, \dots, \bar{f}_n\}$ forms a basis of $\mathbb{Z}_p^n$. Then by the well-known Nakayama lemma (see e.g. [11, p. 8, Theorem 2.2]), $f_1, f_2, \dots, f_n$ span $\mathbb{Z}_q^n$. Finally, since $|\sum_{i=1}^n \mathbb{Z}_q f_i| = |\mathbb{Z}_q^n| = q^n$, $f_1, f_2, \dots, f_n$ must be linearly independent over $\mathbb{Z}_q$. This completes the proof of Lemma 1.1. $\square$

Corollary 1.2. *Let x be an element of $\mathbb{Z}_q^n$. Then $\mathbb{Z}_q x$ is a direct summand of $\mathbb{Z}_q^n$ if and only if* $\mathrm{ord}_p^{(r)}(x) = 0$.

Let $B : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \to \mathbb{Z}_q$ be a symmetric bilinear form. For a subset U of $\mathbb{Z}_q^n$, we define the orthogonal complement $U^\perp$ of U by

$$U^\perp = \{x \in \mathbb{Z}_q^n \mid B(x, y) = 0 \text{ for all } y \in U\}.$$

The symmetric bilinear form B is said to be *non-degenerate* if $\det(B(e_i, e_j)) \in \mathbb{Z}_q^\times = \mathbb{Z}_q \backslash p\mathbb{Z}_q$, where $\{e_1, e_2, \dots, e_n\}$ is the standard basis of $\mathbb{Z}_q^n$, that is, e_i is the element of $\mathbb{Z}_q^n$ with 1 in the i-th component and zero elsewhere. Clearly, this condition is equivalent to saying that the map $x \in \mathbb{Z}_q^n \mapsto B(x, \cdot) \in \mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Z}_q^n, \mathbb{Z}_q)$ gives an isomorphism between $\mathbb{Z}_q^n$ and $\mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Z}_q^n, \mathbb{Z}_q)$.

A *quadratic form* on $\mathbb{Z}_q^n$ is a map $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ satisfying

$$f(ax) = a^2 f(x),$$
$$f(x + y) = f(x) + f(y) + B_f(x, y),$$

for any $a \in \mathbb{Z}_q$ and $x, y \in \mathbb{Z}_q^n$, where B_f is a symmetric bilinear form on $\mathbb{Z}_q^n$. Sometimes we call the pair $(\mathbb{Z}_q^n, f)$ a *quadratic module* over $\mathbb{Z}_q$.

Let $(\mathbb{Z}_q^m, f')$ be another quadratic module over $\mathbb{Z}_q$. An *isometry* $\sigma : (\mathbb{Z}_q^n, f) \to (\mathbb{Z}_q^m, f')$ is an injective $\mathbb{Z}_q$-linear map such that $f(x) = f'(\sigma(x))$ for all $x \in \mathbb{Z}_q^n$ and $\sigma(\mathbb{Z}_q^n)$ is a direct summand of $\mathbb{Z}_q^m$. If in addition the isometry σ is a linear isomorphism, then we say that the two quadratic modules $(\mathbb{Z}_q^n, f)$ and $(\mathbb{Z}_q^m, f')$ are *isomorphic*, and write $(\mathbb{Z}_q^n, f) \cong (\mathbb{Z}_q^m, f')$.

The quadratic form f is said to be *non-degenerate* if B_f is non-degenerate. We define the reductions $\bar{f} : \mathbb{Z}_p^n \to \mathbb{Z}_p$ and $\bar{B}_f : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ of f and B_f modulo $p\mathbb{Z}_q$, in an obvious manner.

The *orthogonal group* $O(\mathbb{Z}_q^n, f)$ is the group of all linear transformations on $\mathbb{Z}_q^n$ that fix f, that is,

$$O(\mathbb{Z}_q^n, f) = \{\sigma \in \mathrm{GL}(\mathbb{Z}_q^n) \mid f(\sigma(x)) = f(x) \text{ for all } x \in \mathbb{Z}_q^n\}.$$

Now we classify all non-degenerate quadratic forms on $\mathbb{Z}_q^n$ using the classification of those on $\mathbb{Z}_p^n$. First of all, we prepare two propositions.

Proposition 1.3 (cf. [1, p. 10, Proposition 3.2]). *Let f be a quadratic form on $\mathbb{Z}_q^n$. If W is a direct summand of $\mathbb{Z}_q^n$ such that the restriction $f|_W$ of f to W is non-degenerate, then we have $\mathbb{Z}_q^n = W \perp W^\perp$.*

Proof. For an element x of $\mathbb{Z}_q^n$, define a $\mathbb{Z}_q$-linear map $\varphi_x : W \to \mathbb{Z}_q$ by $\varphi_x(y) = B_f(x, y)$ for $y \in W$. Since $B_f|_W$ is non-degenerate, there exists a unique element z of W such that $\varphi_x(y) = B_f(z, y)$ for all $y \in W$, so that we have $x = z + (x - z) \in W + W^\perp$. Since clearly $W \cap W^\perp = 0$, we obtain the desired result. $\square$

Proposition 1.4 (cf. [1, p. 11, Corollary 3.3]). *Let f be a quadratic form on $\mathbb{Z}_q^n$. Then, for any orthogonal decomposition $\mathbb{Z}_p^n = \overline{W}_1 \perp \overline{W}_2$ with respect to $\bar{f}$ such that the restriction $\bar{f}|_{\overline{W}_1}$ is non-degenerate, there exists an orthogonal decomposition $\mathbb{Z}_q^n = W_1 \perp W_2$ such that $f|_{W_1}$ is non-degenerate and $\overline{W}_i \cong W_i/pW_i$ $(i = 1, 2)$.*

Proof. Let $y_1, y_2, \ldots, y_n$ be a basis of $\mathbb{Z}_p^n$ such that $y_1, y_2, \ldots, y_l$ span $\overline{W}_1$. For each $y_i = (y_{i1}, y_{i2}, \ldots, y_{in})$ $(1 \leqslant i \leqslant n)$, take an element $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ of $\mathbb{Z}_q^n$ such that $y_i = \bar{x}_i$. Since $\det(y_{ij})_{1 \leqslant i,j \leqslant n} \neq 0$, we have $\det(x_{ij})_{1 \leqslant i,j \leqslant n} \in \mathbb{Z}_q^\times$ so that $x_1, x_2, \ldots, x_n$ form a basis of $\mathbb{Z}_q^n$. Put

$$W_1 = \mathbb{Z}_q x_1 \oplus \mathbb{Z}_q x_2 \oplus \cdots \oplus \mathbb{Z}_q x_l.$$

Since $\bar{f}|_{\overline{W}_1}$ is non-degenerate, we have $\det(\bar{B}_f(y_i, y_j))_{1 \leqslant i,j \leqslant l} \neq 0$, from which it follows that $\det(B_f(x_i, x_j))_{1 \leqslant i,j \leqslant l} \in \mathbb{Z}_q^\times$, that is, $f|_{W_1}$ is non-degenerate. Thus, we have $\mathbb{Z}_q^n = W_1 \perp W_2$ by Proposition 1.3 where $W_2 = W_1^\perp$ and clearly, $\overline{W}_i \cong W_i/pW_i$ $(i = 1, 2)$, as desired. $\square$

It is well-known that the non-degenerate quadratic forms over $\mathbb{Z}_p$ are classified as follows:

Theorem 1.5 (cf. [14]). (i) *Suppose $n = 2m$ is even. If p is odd, then there are two inequivalent non-degenerate quadratic forms f_1^+ and f_1^-:*

$$f_1^+(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m},$$
$$f_1^-(x) = x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 - \varepsilon x_{2m}^2$$

for $x = (x_1, x_2, \ldots, x_{2m}) \in \mathbb{Z}_p^{2m}$, *where* ε *is a non-square element of* $\mathbb{Z}_p$.

If $p = 2$, *then there are also two inequivalent non-degenerate quadratic forms* f_1^+ *and* f_1^-:

$$f_1^+(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m},$$
$$f_1^-(x) = x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 + x_{2m-1}x_{2m} + x_{2m}^2$$

for $x = (x_1, x_2, \ldots, x_{2m}) \in \mathbb{Z}_2^{2m}$.

(ii) *Suppose* $n = 2m+1$ *is odd. If* p *is odd, then there are two inequivalent non-degenerate quadratic forms* f_1 *and* f_1':

$$f_1(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2,$$
$$f_1'(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m} + \varepsilon x_{2m+1}^2$$

for $x = (x_1, x_2, \ldots, x_{2m+1}) \in \mathbb{Z}_p^{2m+1}$, *where* ε *is a non-square element of* $\mathbb{Z}_p$, *but their orthogonal groups* $O(\mathbb{Z}_p^{2m+1}, f_1)$ *and* $O(\mathbb{Z}_p^{2m+1}, f_1')$ *are isomorphic.*

If $p = 2$, *then there is no non-degenerate quadratic form on* $\mathbb{Z}_2^{2m+1}$.

Remark 1.6. The definition of non-degeneracy of a quadratic form in this paper is slightly stronger than that in [14]. Namely, if we define the radical $\operatorname{Rad} f$ of a quadratic form f on $\mathbb{Z}_p^n$ by

$$\operatorname{Rad} f = f^{-1}(0) \cap (\mathbb{Z}_p^n)^\perp,$$

then using the terminology in [14], f is said to be non-degenerate if $\operatorname{Rad} f = 0$. Our definition agrees with this unless $p = 2$ and n is odd. If one adopts the definition in [14], then it turns out that there exists exactly one inequivalent non-degenerate quadratic form f_1 on $\mathbb{Z}_2^{2m+1}$:

$$f_1(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2,$$

for $x = (x_1, x_2, \ldots, x_{2m+1}) \in \mathbb{Z}_2^{2m+1}$, which is clearly degenerate in our sense.

For the convenience of the discussion, we call the (free) quadratic module $(\mathbb{Z}_q e_1 \oplus \mathbb{Z}_q e_2, f)$ of rank two with a distinguished basis $\{e_1, e_2\}$ such that $f(e_1) = \alpha$, $f(e_2) = \beta$ and $B_f(e_1, e_2) = 1$, the quadratic module of type $[\alpha, \beta]$. Similarly, we call the quadratic module $(\mathbb{Z}_q e, f)$ of rank one with a distinguished basis $\{e\}$ such that $f(e) = \zeta$, the quadratic module of type $[\zeta]$. In order to find the isomorphisms among these quadratic modules, we need the following lemma.

Lemma 1.7. (i) *If p is odd, then for any $u \in p\mathbb{Z}_q$, there exists a unique element $a \in \mathbb{Z}_q$ such that $a \equiv 1 \bmod p$ and $a^2 - a \equiv u \bmod q$.*

(ii) *If $p = 2$, then for any odd t and even u in $\mathbb{Z}_q$, there exist unique even a and odd b in $\mathbb{Z}_q$ such that $a^2 + ta \equiv b^2 + tb \equiv u \bmod q$.*

Proof. (i) Let a and b be elements of $1 + p\mathbb{Z}_q$. Then we have $a^2 - a \equiv b^2 - b \bmod q$ if and only if $(a-b)(a+b-1) \equiv 0 \bmod q$. Since $a+b-1 \equiv 1 \bmod p$, this implies $a \equiv b \bmod q$. Therefore $a^2 - a$ takes all $u \in p\mathbb{Z}_q$ as a runs through $1 + p\mathbb{Z}_q$.

(ii) The proof is similar to that of (i), hence omitted. □

Using Lemma 1.7, we obtain the following.

Proposition 1.8. (i) *For any α and β in $p\mathbb{Z}_q$, the quadratic modules of type $[\alpha, \beta]$ and $[0, 0]$ are isomorphic.*

(ii) *If $p = 2$, then the quadratic modules of type $[\gamma, \delta]$ and $[1, 1]$ are isomorphic for any γ and δ in $\mathbb{Z}_q^{\times}$.*

(iii) *Suppose p is odd, and let ε be a non-square element of $\mathbb{Z}_p$. Then for each $\zeta \in \mathbb{Z}_q^{\times}$, the quadratic module of type $[\zeta]$ is isomorphic to that of type $[1]$ or $[\varepsilon]$, depending on whether ζ is a square or not.*

Proof. (i) Let $\{e_1, e_2\}$ be the distinguished basis of the quadratic module of type $[0, 0]$. By Proposition 1.7 (i) and (ii), there exists unique $a \in \mathbb{Z}_q$ such that $a \equiv 1 \bmod p$ and $a^2 - a \equiv -\alpha\beta \bmod q$. Put

$$e_1' = ae_1 + a^{[-1]}\alpha e_2 \quad \text{and} \quad e_2' = \beta e_1 + e_2.$$

Then since

$$\det\begin{pmatrix} a & \beta \\ a^{[-1]}\alpha & 1 \end{pmatrix} = a - a^{[-1]}\alpha\beta \equiv 1 \bmod p,$$

$\{e_1', e_2'\}$ therefore forms another basis. Clearly, we have $f(e_1') = \alpha$, $f(e_2') = \beta$ and $B_f(e_1', e_2') = 1$.

(ii) Let $\{e_1, e_2\}$ be the distinguished basis of the quadratic module of type $[1, 1]$. Then it follows from Proposition 1.7 (ii) that there exist a and unique even b in $\mathbb{Z}_q$ such that $a^2 + a \equiv \gamma - 1 \bmod q$ and $3\gamma b^2 - 3b \equiv (2a+1)^2\delta - 1 \bmod q$. Put

$$e_1' = ae_1 + e_2 \quad \text{and} \quad e_2' = (2a+1)^{[-1]}(1 - ab - 2b)e_1 + be_2.$$

Since b is even,

$$\det\begin{pmatrix} a & (2a+1)^{[-1]}(1 - ab - 2b) \\ 1 & b \end{pmatrix}$$

is odd, so that $\{e_1', e_2'\}$ is a basis. First, we have $f(e_1') = a^2 + a + 1 \equiv \gamma \bmod q$. Also, since

$$\begin{aligned}(2a+1)B_f(e_1', e_2') &= 2a(1-ab-2b) + (2a+1)ab + (1-ab-2b) + 2(2a+1)b\\ &= 2a+1,\end{aligned}$$

we have $B_f(e_1', e_2') = 1$. Finally, it follows that

$$\begin{aligned}(2a+1)^2 f(e_2') &= (1-ab-2b)^2 + (2a+1)(1-ab-2b)b + (2a+1)^2 b^2\\ &= 3(a^2+a+1)b^2 - 3b + 1\\ &\equiv 3\gamma b^2 - 3b + 1 \bmod q\\ &\equiv (2a+1)^2\delta \bmod q,\end{aligned}$$

so that $f(e_2') = \delta$.

(iii) This is trivial, since $\mathbb{Z}_q^\times$ is a cyclic group if p is odd. $\square$

Combining Theorem 1.5, Proposition 1.4 and Proposition 1.8, we conclude that:

Theorem 1.9. (i) *Suppose $n = 2m$ is even. If p is odd, then there are two inequivalent non-degenerate quadratic forms f_r^+ and f_r^- on $\mathbb{Z}_q^{2m}$:*

$$\begin{aligned}f_r^+(x) &= x_1x_2 + \cdots + x_{2m-1}x_{2m},\\ f_r^-(x) &= x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 - \varepsilon x_{2m}^2\end{aligned}$$

for $x = (x_1, x_2, \ldots, x_{2m}) \in \mathbb{Z}_q^{2m}$, where ε is a non-square element of $\mathbb{Z}_p$.

If $p = 2$, then there are also two inequivalent non-degenerate quadratic forms f_r^+ and f_r^- on $\mathbb{Z}_q^{2m}$:

$$\begin{aligned}f_r^+(x) &= x_1x_2 + \cdots + x_{2m-1}x_{2m},\\ f_r^-(x) &= x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 + x_{2m-1}x_{2m} + x_{2m}^2\end{aligned}$$

for $x = (x_1, x_2, \ldots, x_{2m}) \in \mathbb{Z}_q^{2m}$.

(ii) *Suppose $n = 2m+1$ is odd. If p is odd, then there are two inequivalent non-degenerate quadratic forms f_r and f_r' on $\mathbb{Z}_q^{2m+1}$:*

$$\begin{aligned}f_r(x) &= x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2,\\ f_r'(x) &= x_1x_2 + \cdots + x_{2m-1}x_{2m} + \varepsilon x_{2m+1}^2\end{aligned}$$

for $x = (x_1, x_2, \ldots, x_{2m+1}) \in \mathbb{Z}_q^{2m+1}$, where ε is a non-square element of $\mathbb{Z}_p$.

If $p = 2$, then there is no non-degenerate quadratic form on $\mathbb{Z}_q^{2m+1}$.

In what follows, we denote the orthogonal groups of f_r^+, f_r^- and f_r by $GO_{2m}^+(\mathbb{Z}_q)$, $GO_{2m}^-(\mathbb{Z}_q)$ and $GO_{2m+1}(\mathbb{Z}_q)$, respectively. It is easy to see that the orthogonal group $O(\mathbb{Z}_q^{2m+1}, f_r')$ is isomorphic to $GO_{2m+1}(\mathbb{Z}_q)$.

2 The character tables

2.1 The relations of $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$. As in the introduction, let $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$ denote the symmetric association scheme obtained from the action of $O(\mathbb{Z}_q^n, f) \ltimes \mathbb{Z}_q^n$ on $\mathbb{Z}_q^n$. That is, the relations of $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$ are the orbits of $O(\mathbb{Z}_q^n, f) \ltimes \mathbb{Z}_q^n$ in its natural action on $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$. Since the stabilizer of an element of $\mathbb{Z}_q^n$ in $O(\mathbb{Z}_q^n, f) \ltimes \mathbb{Z}_q^n$ is isomorphic to $O(\mathbb{Z}_q^n, f)$, the relations of $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$ are in one-to-one correspondence with the orbits of $O(\mathbb{Z}_q^n, f)$ on $\mathbb{Z}_q^n$.

For quadratic modules over fields, there is a very famous theorem known as Witt's extension theorem (see e.g. [14]). Knebusch [9] proved that a similar result also holds for quadratic modules over any local ring. In our case, this result is stated as follows.

Theorem 2.1 ([9, Satz 5.1]). *Let f be a non-degenerate quadratic form on $\mathbb{Z}_q^n$. Suppose that W is a direct summand of $\mathbb{Z}_q^n$ and $\tau : W \to \mathbb{Z}_q^n$ is an isometry. Then there exists an extension $\sigma \in O(\mathbb{Z}_q^n, f)$ of τ, i.e. $\sigma|_W = \tau$.*

We use Theorem 2.1 to determine the relations of $\mathfrak{X}(O(\mathbb{Z}_q^n, f), \mathbb{Z}_q^n)$.

Lemma 2.2. *Let f be a non-degenerate quadratic form on $\mathbb{Z}_q^n$. Then for any element x of $\mathbb{Z}_q^n$ such that $\mathrm{ord}_p^{(r)}(x) = 0$ and $a \in \mathbb{Z}_{p^l}$ $(0 \leqslant l < r)$, there exists an element y of $\mathbb{Z}_q^n$ such that $x \equiv y \bmod p^{r-l}\mathbb{Z}_q^n$ and $f(y) = f(x) + p^{r-l}a$.*

Proof. Since $\bar{B}_f$ is non-degenerate and $\bar{x} \neq \bar{0}$, there exists an element $z \in \mathbb{Z}_q^n$ such that $\bar{B}_f(\bar{x}, \bar{z}) \neq \bar{0}$, or equivalently, $B_f(x, z) \in \mathbb{Z}_q^\times$. Notice that for any $b, c \in \mathbb{Z}_{p^l}$ we have

$$bB_f(x,z) + p^{r-l}b^2 f(z) \equiv cB_f(x,z) + p^{r-l}c^2 f(z) \bmod p^l$$

if and only if

$$(b-c)\{B_f(x,z) + p^{r-l}(b+c)f(z)\} \equiv 0 \bmod p^l.$$

Since $B_f(x,z) + p^{r-l}(b+c)f(z) \not\equiv 0 \bmod p$, this implies $b = c$. Therefore, there exists a unique element c of $\mathbb{Z}_{p^l}$ such that $cB_f(x,z) + p^{r-l}c^2 f(z) \equiv a \bmod p^l$. Clearly, $y = x + p^{r-l}cz \in \mathbb{Z}_q^n$ is a desired element. □

Remark 2.3. In fact, with the notation of Lemma 2.2, the above proof shows the existence of an element $z \in \mathbb{Z}_q^n$ such that for all $v \in \mathbb{Z}_q^n$ with $v \equiv x \bmod p^{r-l}\mathbb{Z}_q^n$, $f(v + p^{r-l}cz)$ $(c \in \mathbb{Z}_{p^l})$ are distinct and

$$\{f(v + p^{r-l}cz) \mid c \in \mathbb{Z}_{p^l}\} = f(x) + p^{r-l}\mathbb{Z}_q.$$

Proposition 2.4. *Let f be a non-degenerate quadratic form on $\mathbb{Z}_q^n$. Then for two non-zero elements x and y of $\mathbb{Z}_q^n$, there exists an automorphism $\sigma \in O(\mathbb{Z}_q^n, f)$ such that $\sigma(x) = y$ if and only if $\mathrm{ord}_p^{(r)}(x) = \mathrm{ord}_p^{(r)}(y)$ and $f\left(\frac{1}{p^l}x\right) \equiv f\left(\frac{1}{p^l}y\right) \bmod p^{r-l}$ where $l = \mathrm{ord}_p^{(r)}(x)$.*

Proof. The "only if" part is obvious. Assume $l = \mathrm{ord}_p^{(r)}(x) = \mathrm{ord}_p^{(r)}(y)$ $(< r)$ and $f\left(\frac{1}{p^l}x\right) \equiv f\left(\frac{1}{p^l}y\right) \bmod p^{r-l}$. Then by Lemma 2.2, there exists an element u of $\mathbb{Z}_q^n$ such that $u \equiv \frac{1}{p^l}x \bmod p^{r-l}\mathbb{Z}_{p^l}^n$ and $f(u) = f\left(\frac{1}{p^l}y\right)$. Since $\mathbb{Z}_q u$ and $\mathbb{Z}_q \frac{1}{p^l}y$ are direct summands of $\mathbb{Z}_q^n$ by Corollary 1.2, it follows from Theorem 2.1 that there exists $\sigma \in O(\mathbb{Z}_q^n, f)$ such that $\sigma(u) = \frac{1}{p^l}y$. Then we have $\sigma(x) = p^l\sigma(u) = y$. □

In the next subsection, we calculate the character table of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$. The discussions are almost parallel to those in Medrano et al. [13] and DeDeo [8]. In §2.3 and §2.4, the results for $\mathfrak{X}(GO_{2m}^+(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ and $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ are stated without detailed proofs.

2.2 The character table of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$. By Proposition 2.4, the relations of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ are given as follows.

$$(x, y) \in R_0^{(r)} \Leftrightarrow x = y,$$
$$(x, y) \in R_{l,a}^{(r)} \Leftrightarrow x - y \in \Lambda_{l,a}^{(r)}$$

for $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$, where $\Lambda_{l,a}^{(r)}$ is an orbit of $GO_{2m}^-(\mathbb{Z}_q)$ on $\mathbb{Z}_q^{2m}$ defined by

$$\begin{aligned}\Lambda_{l,a}^{(r)} &= \left\{x \in \mathbb{Z}_q^{2m} \mid \mathrm{ord}_p^{(r)}(x) = l, f_r^-\left(\frac{1}{p^l}x\right) \equiv a \bmod p^{r-l}\right\}\\ &= \{p^l u \mid u \in \Lambda_{0,a}^{(r-l)}\}.\end{aligned}$$

Notice that the $k_{l,a}^{(r)} = |\Lambda_{l,a}^{(r)}|$ are the valencies of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$.

Proposition 2.5. *For $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$, we have*

$$k_{l,a}^{(r)} = |\Lambda_{l,a}^{(r)}| = \begin{cases} p^{(r-l-1)(2m-1)} \cdot p^{m-1}(p^m + 1), & \text{if } p \nmid a, \\ p^{(r-l-1)(2m-1)} \cdot (p^{m-1} - 1)(p^m + 1), & \text{if } p \mid a. \end{cases}$$

In particular, $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ is a symmetric association scheme of class

$$p^r + p^{r-1} + \cdots + p = \frac{p(p^r - 1)}{p - 1}$$

if $m > 1$, and of class

$$(p^r - p^{r-1}) + (p^{r-1} - p^{r-2}) + \cdots + (p - 1) = p^r - 1$$

if $m = 1$.

Proof. Since $|\Lambda_{l,a}^{(r)}| = |\Lambda_{0,a}^{(r-l)}|$, we only have to prove the equality when $l = 0$. If $r = 1$, then it is easy to see that the assertion is true (cf. [10, §3.3]). Now, suppose $r > 1$. Then for an element x of $\mathbb{Z}_q^{2m}$, we have $\mathrm{ord}_p^{(r)}(x) = 0$ if and only if $\bar{x} \neq \bar{0}$, from which it follows that

$$\begin{aligned} &|\{x \in \mathbb{Z}_q^{2m} \mid \mathrm{ord}_p^{(r)}(x) = 0, f_r^-(x) \equiv a \bmod p\}| \\ &\quad = \begin{cases} p^{(r-1)2m} \cdot p^{m-1}(p^m + 1), & \text{if } p \nmid a, \\ p^{(r-1)2m} \cdot (p^{m-1} - 1)(p^m + 1), & \text{if } p \mid a. \end{cases} \end{aligned} \tag{1}$$

By Remark 2.3, $|\Lambda_{0,a}^{(r)}|$ is obtained by dividing the right-hand side of (1) by p^{r-1}. □

Medrano et al. [13] and DeDeo [8] determined the graph spectra of the graphs $(R_{0,a}^{(r)}, \mathbb{Z}_q^{2m})$ $(a \in \mathbb{Z}_q^{\times})$ completely for many cases. We apply this method in the calculation of the character table of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$.

Let $V^{(r)}$ be the complex vector space of the functions $\varphi : \mathbb{Z}_q^{2m} \to \mathbb{C}$. For each $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$, we define the *adjacency operator* $A_{l,a}^{(r)}$ on $V^{(r)}$ by

$$A_{l,a}^{(r)}\varphi(x) = \sum_{x-y \in \Lambda_{l,a}^{(r)}} \varphi(y)$$

for all $\varphi \in V^{(r)}$. We will decompose $V^{(r)}$ into the direct sum of the maximal common eigenspaces of the $A_{l,a}^{(r)}$'s.

For brevity, we denote the associated bilinear form $B_{f_r^-}$ of f_r^- simply by B_r^-. Also, we use the notation

$$e^{(r)}(a) = \exp(2\pi\sqrt{-1}a/p^r)$$

for $a \in \mathbb{Z}_q$. For each $u \in \mathbb{Z}_q^{2m}$, define a linear character $e_u^{(r)} : \mathbb{Z}_q^{2m} \to \mathbb{C}$ by

$$e_u^{(r)}(x) = e^{(r)}(B_r^-(u, x))$$

for $x \in \mathbb{Z}_q^{2m}$. Then, since B_r^- is non-degenerate, the $e_u^{(r)}$'s are distinct and they form an orthonormal basis of $V^{(r)}$ with respect to the inner product

$$(\varphi, \psi) = \frac{1}{q^{2m}} \sum_{x \in \mathbb{Z}_q^{2m}} \varphi(x)\overline{\psi(x)}$$

on $V^{(r)}$.

Proposition 2.6 (cf. [13, Proposition 2.2]). *For each element u of $\mathbb{Z}_q^{2m}$, the function $e_u^{(r)}$ is a common eigenfunction of the $A_{l,a}^{(r)}$'s, and the eigenvalue of $A_{l,a}^{(r)}$ corresponding to $e_u^{(r)}$ is given by*

$$\lambda_{l,a,u}^{(r)} = \sum_{z \in \Lambda_{l,a}^{(r)}} e_u^{(r)}(z). \tag{2}$$

Proof. Note that

$$A_{l,a}^{(r)} e_u^{(r)}(x) = \sum_{x-y \in \Lambda_{l,a}^{(r)}} e_u^{(r)}(y) = \sum_{z \in \Lambda_{l,a}^{(r)}} e_u^{(r)}(x+z) = \left(\sum_{z \in \Lambda_{l,a}^{(r)}} e_u^{(r)}(z) \right) e_u^{(r)}(x). \qquad \square$$

Our next problem is to evaluate the eigenvalues $\lambda_{l,a,u}^{(r)}$.

Proposition 2.7 (cf. [13, Theorem 2.3]). (i) *For $0 \leqslant l < r$, $a \in \mathbb{Z}_{p^{r-l}}$ and $u \in \mathbb{Z}_q^{2m}$, we have $\lambda_{l,a,u}^{(r)} = \lambda_{0,a,u}^{(r-l)}$.*

(ii) *For $a \in \mathbb{Z}_q$ and $u \in \mathbb{Z}_q^{2m}$, we have*

$$\lambda_{0,a,u}^{(r)} = \begin{cases} |\Lambda_{0,a}^{(r)}|, & \text{if } u = 0, \\ p^{k(2m-1)} \lambda_{0,a,(1/p^k)u}^{(r-k)}, & \text{if } u \neq 0, \end{cases}$$

where $k = \mathrm{ord}_p^{(r)}(u)$.

Proof. (i) This is clear from the definition of $\Lambda_{l,a}^{(r)}$.

(ii) The assertion is trivial when $k = 0$ or $k = r$ (i.e. $u = 0$) therefore, we assume $1 \leqslant k < r$, so that $r \geqslant 2$.

We write $a = a' + p^{r-1}a''$, with $a' \in \mathbb{Z}_{p^{r-1}}$ and $a'' \in \mathbb{Z}_p$. For each $z = z' + p^{r-1}z'' \in \mathbb{Z}_q^{2m}$ with $z' \in \mathbb{Z}_{p^{r-1}}^{2m}$ and $z'' \in \mathbb{Z}_p^{2m}$, we have

$$f_r^-(z) \equiv f_r^-(z') + p^{r-1} B_r^-(z', z'') \bmod p^r,$$

since $r \geqslant 2$. Now, let

$$M = \{ z' \in \mathbb{Z}_{p^{r-1}}^{2m} \mid \mathrm{ord}_p^{(r-1)}(z') = 0, f_r^-(z') \equiv a' \bmod p^{r-1} \},$$

and for each $z' \in M$ let

$$N(z') = \{ z'' \in \mathbb{Z}_p^{2m} \mid B_r^-(z', z'') \equiv a'' - y \bmod p \}$$

where $f_r^-(z') = a' + p^{r-1}y$ with $y \in \mathbb{Z}_p$. Then since $z' \not\equiv 0 \bmod p$ and $B_1^- = \overline{B}_r^-$ is non-degenerate, we have $|N(z')| = p^{2m-1}$, from which it follows that

$$\begin{aligned}\lambda^{(r)}_{0,a,u} &= \sum_{z'\in M}\sum_{z''\in N(z')} e^{(r)}_u(z' + p^{r-1}z'') \\ &= \sum_{z'\in M}\sum_{z''\in N(z')} e^{(r)}\left(B^-_r\left(p\cdot\frac{1}{p}u, z' + p^{r-1}z''\right)\right) \\ &= p^{2m-1}\lambda^{(r-1)}_{0,a,(1/p)u}.\end{aligned}$$

By repeating the same argument, we obtain the desired result. □

By virtue of Proposition 2.7, we only have to evaluate $\lambda^{(r)}_{0,a,u}$ for $u \in \mathbb{Z}_q^{2m}$ with $\mathrm{ord}_p^{(r)}(u) = 0$.

In the case of fields, the character tables of the association schemes of affine type are described by using the Kloosterman sums ([12], [5]). In the process of studying $\lambda^{(r)}_{0,a,u}$, we will encounter the Kloosterman sums over rings. Let κ be a linear character of the multiplicative group $\mathbb{Z}_q^\times$. Then for $a, b \in \mathbb{Z}_q$, we define the *Kloosterman sum* $K^{(r)}(\kappa \mid a, b)$ by

$$K^{(r)}(\kappa \mid a, b) = \sum_{\gamma\in\mathbb{Z}_q^\times} \kappa(\gamma)e^{(r)}(a\gamma + b\gamma^{[-1]}).$$

Note that these sums are completely evaluated by Salié [15] when $r > 1$ and $\kappa = 1$ (see also [8]).

We shall need to evaluate the following exponential sum:

$$\Omega^{(r)}_\gamma = \sum_{v\in\mathbb{Z}_q^{2m}} e^{(r)}(f_r^-(v)\gamma)$$

for $\gamma \in \mathbb{Z}_q^\times$.

Proposition 2.8. *For any element γ of $\mathbb{Z}_q^\times$, we have $\Omega^{(r)}_\gamma = (-1)^r q^m$.*

Proof. First of all, it is easy to see that

$$\sum_{v_1, v_2\in\mathbb{Z}_q} e^{(r)}(v_1v_2\gamma) = q.$$

Therefore, if p is odd, then we have to show that

$$\sum_{v_1, v_2\in\mathbb{Z}_q} e^{(r)}((v_1^2 - \varepsilon v_2^2)\gamma) = (-1)^r q,$$

where, as usual, ε is a non-square element in $\mathbb{Z}_p^\times$. However, this equality directly follows from the evaluation of the Gauss sums (cf. [6, p. 26, Theorem 1.5.2], see also [13, Corollary 2.7]):

$$g(i;h) = \sum_{j=0}^{h-1} \exp(2\pi\sqrt{-1}\, ij^2/h) = \begin{cases} \left(\dfrac{i}{h}\right)\sqrt{h}, & \text{if } h \equiv 1 \bmod 4, \\ \left(\dfrac{i}{h}\right)\sqrt{-h}, & \text{if } h \equiv 3 \bmod 4, \end{cases} \tag{3}$$

where i and h are any coprime integers with $h > 0$ and h odd, and $\left(\frac{s}{h}\right)$ is the Jacobi symbol.

If $p = 2$, then in this case we have to show that

$$\omega_\gamma^{(r)} = \sum_{v_1, v_2 \in \mathbb{Z}_q} e^{(r)}((v_1^2 + v_1 v_2 + v_2^2)\gamma) = (-1)^r q. \tag{4}$$

Now, let v_1 be an odd element of $\mathbb{Z}_q$. Then, by Lemma 1.7 (ii) it follows that

$$\{v_1 v_2 + v_2^2 \mid v_2 : \text{odd}\} = \{v_1 v_2 + v_2^2 \mid v_2 : \text{even}\} = 2\mathbb{Z}_q,$$

so that if $r > 1$, then we have

$$\sum_{v_2 : \text{odd}} e^{(r)}((v_1^2 + v_1 v_2 + v_2^2)\gamma) = \sum_{v_2 : \text{even}} e^{(r)}((v_1^2 + v_1 v_2 + v_2^2)\gamma) = 0.$$

In this way, we obtain

$$\omega_\gamma^{(r)} = \sum_{w_1, w_2 \in \mathbb{Z}_{2^{r-1}}} e^{(r)}(4(w_1^2 + w_1 w_2 + w_2^2)\gamma) = 4\omega_\gamma^{(r-2)},$$

if $r \geqslant 3$. Therefore, (4) follows from an easy calculation:

$$\omega_\gamma^{(1)} = -2, \quad \omega_\gamma^{(2)} = 4.$$

This completes the proof of Proposition 2.8. □

Theorem 2.9 (cf. [13, Theorem 2.9]). *Let a be an element of $\mathbb{Z}_q$. Then for any $u \in \mathbb{Z}_q^{2m}$ with $\mathrm{ord}_p^{(r)}(u) = 0$, we have the following.*

(i) *If $r > 1$, then we have*

$$\lambda_{0,a,u}^{(r)} = (-1)^r p^{r(m-1)} K^{(r)}(1 \mid a, f_r^-(u)).$$

(ii) *If $r = 1$, then we have*

$$\lambda_{0,a,u}^{(1)} = -p^{m-1}K^{(1)}(1 \mid a, f_1^-(u)) - \delta_0(a)$$

where $\delta_b(a)$ *is defined by*

$$\delta_b(a) = \begin{cases} 1 & \text{if } a \equiv b \bmod p, \\ 0 & \text{if } a \not\equiv b \bmod p. \end{cases}$$

Proof. We regard $\lambda_{0,a,u}^{(r)}$ as a function in a, then it has the Fourier expansion with respect to the linear characters $\{e^{(r)}(a\gamma)\}_{\gamma \in \mathbb{Z}_q}$ of $\mathbb{Z}_q$:

$$\lambda_{0,a,u}^{(r)} = \frac{1}{q} \sum_{\gamma \in \mathbb{Z}_q} C_\gamma^{(r)}(u) e^{(r)}(-a\gamma)$$

for all $a \in \mathbb{Z}_q$, where the coefficients $C_\gamma^{(r)}(u)$ are given by

$$C_\gamma^{(r)}(u) = \sum_{b \in \mathbb{Z}_q} \lambda_{0,b,u}^{(r)} e^{(r)}(b\gamma) = \sum_{\substack{z \in \mathbb{Z}_q^{2m} \\ \mathrm{ord}_p^{(r)}(z)=0}} e^{(r)}(B_r^-(u,z) + f_r^-(z)\gamma)$$

We write

$$\lambda_{0,a,u}^{(r)} = \frac{1}{q}\left(\sum\nolimits_1 + \sum\nolimits_2\right), \tag{5}$$

where

$$\sum\nolimits_1 = \sum_{p \mid \gamma} C_\gamma^{(r)}(u) e^{(r)}(-a\gamma), \quad \sum\nolimits_2 = \sum_{p \nmid \gamma} C_\gamma^{(r)}(u) e^{(r)}(-a\gamma).$$

First of all, assume $r > 1$. We evaluate $\sum_1$. Setting $\gamma = p\zeta$ with $\zeta \in \mathbb{Z}_{p^{r-1}}$, we obtain

$$\begin{aligned} \sum\nolimits_1 &= \sum_{\substack{z \in \mathbb{Z}_q^{2m} \\ \mathrm{ord}_p^{(r)}(z)=0}} e_u^{(r)}(z) \sum_{\zeta \in \mathbb{Z}_{p^{r-1}}} e^{(r-1)}((f_r^-(z) - a)\zeta) \\ &= p^{r-1} \sum_z e_u^{(r)}(z) \end{aligned}$$

summed over $z \in \mathbb{Z}_q^{2m}$ such that $\mathrm{ord}_p^{(r)}(z) = 0$ and $f_r^-(z) \equiv a \bmod p^{r-1}$. If we let $z = z' + p^{r-1}z''$ with $z \in \mathbb{Z}_{p^{r-1}}^{2m}$ and $z'' \in \mathbb{Z}_p^{2m}$, then this sum is equal to

$$p^{r-1} \sum_{z'} e_u^{(r)}(z') \sum_{z'' \in \mathbb{Z}_p^{2m}} e^{(1)}(B_r^-(u, z'')),$$

where the first sum is over $z' \in \mathbb{Z}_{p^{r-1}}$ such that $\mathrm{ord}_p^{(r-1)}(z') = 0$ and $f_{r-1}^-(z') \equiv a \bmod p^{r-1}$. Since $\mathrm{ord}_p^{(r)}(u) = 0$, this is in turn equal to 0.

Now, we evaluate $\sum_2$. Since $B_r^-(u,z) + f_r^-(z)\gamma = f_r^-(z + \gamma^{[-1]}u)\gamma - f_r^-(u)\gamma^{[-1]}$ if $p \nmid \gamma$, we have

$$\sum\nolimits_2 = \sum_{p \nmid \gamma} \left\{ \sum_v e^{(r)}(f_r^-(v)\gamma) \right\} e^{(r)}(-a\gamma - f_r^-(u)\gamma^{[-1]}),$$

where the inner sum on the right is over $v \in \mathbb{Z}_q^{2m}$ such that $v \not\equiv \gamma^{[-1]}u \bmod p\mathbb{Z}_q^{2m}$. However, since $r > 1$, it follows from Remark 2.3 that

$$\sum_v e^{(r)}(f_r^-(v)\gamma) = 0,$$

where the sum on the left is over $v \in \mathbb{Z}_q^{2m}$ such that $v \equiv \gamma^{[-1]}u \bmod p\mathbb{Z}_q^{2m}$. Hence, we have

$$\sum\nolimits_2 = \sum_{p \nmid \gamma} \Omega_\gamma^{(r)} e^{(r)}(-a\gamma - f_r^-(u)\gamma^{[-1]}) = (-1)^r q^m K^{(r)}(1 \,|\, a, f_r^-(u)),$$

by Proposition 2.8.

By substituting the above evaluations to (5), we conclude that the eigenvalue $\lambda_{0,a,u}^{(r)}$ is written in the desired form.

Finally, when $r = 1$, we can evaluate $\lambda_{0,a,u}^{(1)}$ in exactly the same way, but we omit the details. □

To summarize:

Theorem 2.10. *For $0 \leqslant k < r$ and $b \in \mathbb{Z}_{p^{r-k}}$, let*

$$V_{k,b}^{(r)} = \bigoplus_{u \in \Lambda_{k,b}^{(r)}} \mathbb{C} e_u^{(r)}.$$

Then $V_{k,b}^{(r)}$ is a maximal common eigenspace of the adjacency operators $A_{l,a}^{(r)}$ $(0 \leqslant l < r,\ a \in \mathbb{Z}_{p^{r-l}})$. Moreover, we have the direct sum decomposition:

$$V^{(r)} = V_0^{(r)} \oplus \bigoplus_{\substack{0 \leqslant k < r \\ b \in \mathbb{Z}_{p^{r-k}}}} V_{k,b}^{(r)},$$

where $V_0^{(r)} = \mathbb{C} e_0^{(r)}$ is the trivial maximal common eigenspace. With these parameterizations, the $(k,b;l,a)$-entry $p_{l,a}^{(r)}(k,b)$ of the character table $P(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ (i.e. the eigenvalue of $A_{l,a}^{(r)}$ corresponding to $V_{k,b}^{(r)}$) is given by

$$p_{l,a}^{(r)}(k,b) = \begin{cases} p^{k(2m-1)} \cdot (-1)^{r-k-l} p^{(r-k-l)(m-1)} K^{(r-k-l)}(1 \mid a,b), & \textit{if } k+l < r-1, \\ -p^{k(2m-1)} \cdot \{p^{m-1} K^{(1)}(1 \mid a,b) + \delta_0(a)\}, & \textit{if } k+l = r-1, \\ p^{(r-l-1)(2m-1)} \cdot p^{m-1}(p^m+1), & \textit{if } k+l \geqslant r \textit{ and } p \nmid a, \\ p^{(r-l-1)(2m-1)} \cdot (p^{m-1}-1)(p^m+1), & \textit{if } k+l \geqslant r \textit{ and } p \mid a. \end{cases}$$

In particular, $\mathfrak{X}(GO_{2m}^{-}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ *is self-dual.*

Proof. All but the last statement follow from the above calculations. Obviously, $x \mapsto e_x^{(r)}$ $(x \in \mathbb{Z}_q^{2m})$ defines an isomorphism between $\mathfrak{X}(GO_{2m}^{-}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ and its dual. $\square$

Example 2.11. The character table $P = P(GO_{2m}^{-}(\mathbb{Z}_4), \mathbb{Z}_4^{2m})$ of $\mathfrak{X}(GO_{2m}^{-}(\mathbb{Z}_4), \mathbb{Z}_4^{2m})$ $(m > 1)$ is given by

$$P = \begin{pmatrix} 1 & 2^{3m-2}(2^m+1) & 2^{2m-1}(2^{m-1}-1)(2^m+1) & 2^{3m-2}(2^m+1) \\ 1 & -2^{2m-1} & 0 & 2^{2m-1} \\ 1 & 0 & 2^{2m-1} & 0 \\ 1 & 2^{2m-1} & 0 & -2^{2m-1} \\ 1 & 0 & -2^{2m-1} & 0 \\ 1 & -2^{3m-2} & 2^{2m-1}(2^{m-1}-1) & -2^{3m-2} \\ 1 & 2^{3m-2} & -2^{2m-1}(2^{m-1}+1) & 2^{3m-2} \end{pmatrix.$$
$$\begin{matrix} 2^{2m-1}(2^{m-1}-1)(2^m+1) & 2^{m-1}(2^m+1) & (2^{m-1}-1)(2^m+1) \\ 0 & -2^{m-1} & 2^{m-1}-1 \\ -2^{2m-1} & 2^{m-1} & -2^{m-1}-1 \\ 0 & -2^{m-1} & 2^{m-1}-1 \\ 2^{2m-1} & 2^{m-1} & -2^{m-1}-1 \\ 2^{2m-1}(2^{m-1}-1) & 2^{m-1}(2^m+1) & (2^{m-1}-1)(2^m+1) \\ -2^{2m-1}(2^{m-1}+1) & 2^{m-1}(2^m+1) & (2^{m-1}-1)(2^m+1) \end{matrix}\Bigg),$$

where the row and column indices are ordered as $(0), (0,1), (0,2), (0,3), (0,0), (1,1), (1,0)$.

2.3 The character table of $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$. It follows from Proposition 2.4 that the relations of $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ are given as follows.

$$(x, y) \in R_0^{(r)} \Leftrightarrow x = y,$$
$$(x, y) \in R_{l,a}^{(r)} \Leftrightarrow x - y \in \Pi_{l,a}^{(r)}$$

for $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$, where $\Pi_{l,a}^{(r)}$ is an orbit of $GO_{2m}^{+}(\mathbb{Z}_q)$ on $\mathbb{Z}_q^{2m}$ defined by

$$\Pi_{l,a}^{(r)} = \left\{ x \in \mathbb{Z}_q^{2m} \mid \mathrm{ord}_p^{(r)}(x) = l, f_r^{+}\left(\frac{1}{p^l}x\right) \equiv a \bmod p^{r-l} \right\}$$
$$= \{ p^l u \mid u \in \Pi_{0,a}^{(r-l)} \}.$$

The valencies $k_{l,a}^{(r)} = |\Pi_{l,a}^{(r)}|$ are given by

$$k_{l,a}^{(r)} = |\Pi_{l,a}^{(r)}| = \begin{cases} p^{(r-l-1)(2m-1)} \cdot p^{m-1}(p^m - 1), & \text{if } p \nmid a, \\ p^{(r-l-1)(2m-1)} \cdot (p^{m-1}+1)(p^m - 1), & \text{if } p \mid a, \end{cases}$$

for $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$. In particular, $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ is a symmetric association scheme of class

$$p^r + p^{r-1} + \cdots + p = \frac{p(p^r - 1)}{p - 1}.$$

Theorem 2.12. *The association scheme $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ is self-dual. For $k, l \in \{0, 1, \ldots, r-1\}$, $a \in \mathbb{Z}_{p^{r-l}}$ and $b \in \mathbb{Z}_{p^{r-k}}$, the $(k, b; l, a)$-entry $p_{l,a}^{(r)}(k, b)$ of the character table $P(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ of $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ is given by*

$$p_{l,a}^{(r)}(k, b) = \begin{cases} p^{k(2m-1)} \cdot p^{(r-k-l)(m-1)} K^{(r-k-l)}(1 \mid a, b), & \text{if } k + l < r - 1, \\ p^{k(2m-1)} \cdot \{ p^{m-1} K^{(1)}(1 \mid a, b) - \delta_0(a) \}, & \text{if } k + l = r - 1, \\ p^{(r-l-1)(2m-1)} \cdot p^{m-1}(p^m - 1), & \text{if } k + l \geqslant r \text{ and } p \nmid a, \\ p^{(r-l-1)(2m-1)} \cdot (p^{m-1}+1)(p^m - 1), & \text{if } k + l \geqslant r \text{ and } p \mid a. \end{cases}$$

Example 2.13. The character table $P = P(GO_{2m}^{+}(\mathbb{Z}_4), \mathbb{Z}_4^{2m})$ of $\mathfrak{X}(GO_{2m}^{+}(\mathbb{Z}_4), \mathbb{Z}_4^{2m})$ is given by

$$P = \begin{pmatrix} 1 & 2^{3m-2}(2^m - 1) & 2^{2m-1}(2^{m-1}+1)(2^m - 1) & 2^{3m-2}(2^m - 1) & 2^{2m-1}(2^{m-1}+1)(2^m - 1) & 2^{m-1}(2^m - 1) & (2^{m-1}+1)(2^m - 1) \\ 1 & -2^{2m-1} & 0 & 2^{2m-1} & 0 & 2^{m-1} & -2^{m-1} - 1 \\ 1 & 0 & 2^{2m-1} & 0 & -2^{2m-1} & -2^{m-1} & 2^{m-1} - 1 \\ 1 & 2^{2m-1} & 0 & -2^{2m-1} & 0 & 2^{m-1} & -2^{m-1} - 1 \\ 1 & 0 & -2^{2m-1} & 0 & 2^{2m-1} & -2^{m-1} & 2^{m-1} - 1 \\ 1 & 2^{3m-2} & -2^{2m-1}(2^{m-1}+1) & 2^{3m-2} & -2^{2m-1}(2^{m-1}+1) & 2^{m-1}(2^m - 1) & (2^{m-1}+1)(2^m - 1) \\ 1 & -2^{3m-2} & 2^{2m-1}(2^{m-1}-1) & -2^{3m-2} & 2^{2m-1}(2^{m-1}-1) & 2^{m-1}(2^m - 1) & (2^{m-1}+1)(2^m - 1) \end{pmatrix},$$

where the row and column indices are ordered as (0), (0,1), (0,2), (0,3), (0,0), (1,1), (1,0).

Remark 2.14. We can observe that the character tables of $\mathfrak{X}(GO_{2m}^-(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ and $\mathfrak{X}(GO_{2m}^+(\mathbb{Z}_q), \mathbb{Z}_q^{2m})$ are closely related with each other. In the case of fields, the character table of $\mathfrak{X}(GO_{2m}^+(\mathbb{F}_q), \mathbb{F}_q^{2m})$ is obtained from that of $\mathfrak{X}(GO_{2m}^-(\mathbb{F}_q), \mathbb{F}_q^{2m})$ essentially by the replacement $q^{m-1} \mapsto -q^{m-1}$ (see [10]). In [4], this phenomenon was called an Ennola type duality. The situation is slightly complicated, but it seems possible to regard our examples as a variation of Ennola type duality.

2.4 The character table of $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$, with q odd. In this subsection, we always assume that $q = p^r$ is odd. The relations of the association scheme $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ are given as follows.

$$(x, y) \in R_0^{(r)} \Leftrightarrow x = y,$$
$$(x, y) \in R_{l,a}^{(r)} \Leftrightarrow x - y \in \Xi_{l,a}^{(r)}$$

for $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$, where $\Xi_{l,a}^{(r)}$ is an orbit of $GO_{2m+1}(\mathbb{Z}_q)$ on $\mathbb{Z}_q^{2m+1}$ defined by

$$\begin{aligned}\Xi_{l,a}^{(r)} &= \left\{x \in \mathbb{Z}_q^{2m+1} \mid \mathrm{ord}_p^{(r)}(x) = l, f_r\left(\frac{1}{p^l}x\right) \equiv a \bmod p^{r-l}\right\} \\ &= \{p^l u \mid u \in \Xi_{0,a}^{(r-l)}\}.\end{aligned}$$

The valencies $k_{l,a}^{(r)} = |\Xi_{l,a}^{(r)}|$ are given by

$$k_{l,a}^{(r)} = |\Xi_{l,a}^{(r)}| = \begin{cases} p^{(r-l-1)2m} \cdot p^m(p^m+1), & \text{if } p \nmid a \text{ and } a : \text{square}, \\ p^{(r-l-1)2m} \cdot p^m(p^m-1), & \text{if } p \nmid a \text{ and } a : \text{nonsquare}, \\ p^{(r-l-1)2m} \cdot (p^{2m}-1), & \text{if } p \mid a \end{cases} \tag{6}$$

for $0 \leqslant l < r$ and $a \in \mathbb{Z}_{p^{r-l}}$. In particular, $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ is a symmetric association scheme of class

$$p^r + p^{r-1} + \cdots + p = \frac{p(p^r-1)}{p-1}.$$

Let χ be the quadratic character of $\mathbb{Z}_p^\times$, that is, $\chi(a) = \left(\frac{a}{p}\right)$ for $a \in \mathbb{Z}_p^\times$. Then, we have the following:

Theorem 2.15. *The association scheme $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ is self-dual. For $k, l \in \{0, 1, \ldots, r-1\}$, $a \in \mathbb{Z}_{p^{r-l}}$ and $b \in \mathbb{Z}_{p^{r-k}}$, the $(k, b; l, a)$-entry $p_{l,a}^{(r)}(k, b)$ of the character table $P(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ of $\mathfrak{X}(GO_{2m+1}(\mathbb{Z}_q), \mathbb{Z}_q^{2m+1})$ is given as follows.*

(i) *If $p \equiv 1 \bmod 4$, then*

$$p_{l,a}^{(r)}(k,b) = \begin{cases} p^{2km} \cdot p^{(r-k-l)(2m-1)/2} K^{(r-k-l)}(1 \mid a,b), & \textit{if } k+l < r-1 \\ & \textit{and } r-k-l : \textit{even}, \\ p^{2km} \cdot p^{(r-k-l)(2m-1)/2} K^{(r-k-l)}(\chi \mid a,b), & \textit{if } k+l < r-1 \\ & \textit{and } r-k-l : \textit{odd}, \\ p^{2km} \cdot \{p^{(2m-1)/2} K^{(1)}(\chi \mid a,b) - \delta_0(a)\}, & \textit{if } k+l = r-1, \\ k_{l,a}^{(r)}, & \textit{if } k+l \geqslant r, \end{cases}$$

where $k_{l,a}^{(r)}$ *is defined in* (6).

(ii) *If* $p \equiv 3 \bmod 4$, *then*

$$p_{l,a}^{(r)}(k,b) = \begin{cases} p^{2km} \cdot p^{(r-k-l)(2m-1)/2} K^{(r-k-l)}(1 \mid a,b), & \textit{if } k+l < r-1 \textit{ and} \\ & r-k-l : \textit{even}, \\ -p^{2km} \cdot \sqrt{-1} p^{(r-k-l)(2m-1)/2} K^{(r-k-l)}(\chi \mid a,b), & \textit{if } k+l < r-1 \textit{ and} \\ & r-k-l : \textit{odd}, \\ -p^{2km} \cdot \{\sqrt{-1} p^{(2m-1)/2} K^{(1)}(\chi \mid a,b) + \delta_0(a)\}, & \textit{if } k+l = r-1, \\ k_{l,a}^{(r)}, & \textit{if } k+l \geqslant r. \end{cases}$$

References

[1] R. Baeza, *Quadratic forms over semilocal rings*. Springer 1978. MR 58 #10972 Zbl 0382.10014

[2] E. Bannai, Character tables of commutative association schemes. In: *Finite geometries, buildings, and related topics* (*Pingree Park, CO*, 1988), 105–128, Oxford Univ. Press 1990. MR 91k:20010 Zbl 0757.05100

[3] E. Bannai, T. Ito, *Algebraic combinatorics. I*. Benjamin/Cummings Publishing Co. 1984. MR 87m:05001 Zbl 0555.05019

[4] E. Bannai, W. M. Kwok, S.-Y. Song, Ennola type dualities in the character tables of some association schemes. *Mem. Fac. Sci. Kyushu Univ. Ser. A* **44** (1990), 129–143. MR 92d:05180 Zbl 0808.20011

[5] E. Bannai, O. Shimabukuro, H. Tanaka, Finite Euclidean graphs and Ramanujan graphs. To appear in *Discrete Math.*

[6] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*. Wiley-Interscience 1998. MR 99d:11092 Zbl 0906.11001

[7] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*. Springer 1989. MR 90e:05001 Zbl 0747.05073

[8] M. R. DeDeo, Graphs over the ring of integers modulo 2^r. PhD thesis, U.C.S.D., CA, 1998.

[9] M. Knebusch, Isometrien über semilokalen Ringen. *Math. Z.* **108** (1969), 255–268. MR 40 #5602 Zbl 0188.35502

[10] W. M. Kwok, Character tables of association schemes of affine type. *European J. Combin.* **13** (1992), 167–185. MR 93h:05177 Zbl 0770.05100

[11] H. Matsumura, *Commutative ring theory*. Cambridge Univ. Press 1986. MR 88h:13001 Zbl 0603.13001

[12] A. Medrano, P. Myers, H. M. Stark, A. Terras, Finite analogues of Euclidean space. *J. Comput. Appl. Math.* **68** (1996), 221–238. MR 97k:11172 Zbl 0874.05030

[13] A. Medrano, P. Myers, H. M. Stark, A. Terras, Finite Euclidean graphs over rings. *Proc. Amer. Math. Soc.* **126** (1998), 701–710. MR 98j:11118 Zbl 0957.05053
[14] A. Munemasa, The geometry of orthogonal groups over finite fields. JSPS-DOST Lecture Notes in Math. **3**, Sophia University, Tokyo, 1996.
[15] H. Salié, Über die Kloostermanschen Summen $S(u, v; q)$. *Math. Z.* **34** (1931), 91–109. Zbl 57.0211.01

Received 31 July, 2002

H. Tanaka, Graduate School of Mathematics, Kyushu University, Hakozaki 6-10-1, Fukuoka, 812-8581, Japan
Email: htanaka@math.kyushu-u.ac.jp