Korean J. Math. **25** (2017), No. 2, pp. 201–209
https://doi.org/10.11568/kjm.2017.25.2.201

THE MASS FORMULA OF SELF-ORTHOGONAL CODES OVER GF(q)

Kwang Ho Kim and Young Ho Park

Abstract. There exists already mass formula which is the number of self orthogonal codes in $GF(q)^n$, but not proof of it. In this paper we described some theories about finite geometry and by using them proved the mass formula when $q = p^m$, p is odd prime.

1. Introduction

Let $GF(q)$ be a finite field. A code C of length n over $GF(q)$ is a subspace of vector space $GF(q)^n$. Euclidean inner product is defined by $\mathbf{u}\cdot\mathbf{v} = \sum u_i v_i$ in $GF(q)^n$. A dual code of C is $C^{\perp} = \{\mathbf{v} \in GF(q)^n | \mathbf{u}\cdot\mathbf{v} = 0 \text{ for all } \mathbf{u} \in C\}$. A code C is called self orthogonal if $C \subset C^{\perp}$. The mass formula about self orthogonal codes over $GF(q)$ is the total number of self orthogonal codes which exist in $GF(q)^n$. This formula has been used in finding mass formula in self orthogonal codes over module Z_{p^n} in [5] [6] or in classification theory [7], etc..This formula is described in paper [2], but no proof is provided. Furthermore we were not able to find the paper [1] in anywhere. So we were courious about the proof and were motivated to begin this research. we have proved mass formula using finite geometry theory. Finite geometry is geometry whose objects are in finite field elements, in particularly is subspace in vector space. In polar space we give algebraic structure to space by using σ-sesquilinear

Received April 5, 2017. Revised May 24, 2017. Accepted May 24, 2017.
2010 Mathematics Subject Classification: 94B05.
Key words and phrases: mass formula, self-orthogonal codes.

form. We introduce finite geometry theories needed to describe the main theorem.

2. Preliminary

2.1. Projective space. Let $V(n+1,q)$ be a vector space of rank n over $GF(q)$. The projective space $PG(n,q)$ is the geometry whose points, lines, planes, ... , hyperplanes are the subspaces of $V(n+1,q)$ of rank $1,2,3,\cdots,n$. In general rank r subspace in projective space is rank $r+1$ subspace in $V(n+1,q)$

2.2. Form. A *σ-sesquilinear form* on $V(n,q)$ is a map

$$\beta : V \times V \longrightarrow GF(q)$$

such that

$$\beta(\mathbf{u}+\mathbf{w},\mathbf{v}) = \beta(\mathbf{u},\mathbf{v}) + \beta(\mathbf{w},\mathbf{v})$$

$$\beta(\mathbf{u},\mathbf{w}+\mathbf{v}) = \beta(\mathbf{u},\mathbf{w}) + \beta(\mathbf{u},\mathbf{v})$$

$$\beta(a\mathbf{u},b\mathbf{v}) = ab^{\sigma}\beta(\mathbf{u},\mathbf{v}),$$

where σ is an automorphism of $GF(q)$. If $\sigma = 1$ then β is called *bilinear*

A form is *degenerate* if there exists a $\mathbf{w} \neq 0$ such that $\beta(\mathbf{u},\mathbf{w}) = 0$ or $\beta(\mathbf{w},\mathbf{u}) = 0$ for all $\mathbf{u} \in V$. A σ-sesquilinear form β is called *reflexive* if $\beta(\mathbf{u},\mathbf{v}) = 0$ implies $\beta(\mathbf{v},\mathbf{u}) = 0$.

THEOREM 2.1. [3] *Let β be a non-denerate σ-sesquilinear form on $V = V(n,q)$. Up to a scalar factor β is one of the following types.*

1. *Alternating form :* $\beta(\mathbf{u},\mathbf{u}) = 0$ *for all* $\mathbf{u} \in V$.
2. *Symmetric form :* $\beta(\mathbf{u},\mathbf{v}) = \beta(\mathbf{v},\mathbf{u})$ *for all* $\mathbf{u},\mathbf{v} \in V$.
3. *Hermitian form :* $\beta(\mathbf{u},\mathbf{v}) = \beta(\mathbf{v},\mathbf{u})^{\sigma}$ *for all* $\mathbf{u},\mathbf{v} \in V$, *where* $\sigma^2 = 1, \sigma \neq 1$

A *quadratic form* on $V(n,q)$ is a function $Q : V(n,q) \longrightarrow GF(q)$ such that

$$Q(a\mathbf{v}) = a^2Q(\mathbf{v}) \quad \text{for all } a \in GF(q),\ \mathbf{v} \in V \quad \textit{and}$$

$$\beta(\mathbf{u},\mathbf{v}) = Q(\mathbf{u}+\mathbf{v}) - Q(\mathbf{u}) - Q(\mathbf{v}) \text{ is a bilinear form.}$$

A quadratic form is *singular* if there exists a $\mathbf{u} \neq 0$ such that $Q(\mathbf{u}) = \beta(\mathbf{u},\mathbf{v}) = 0$ for all $\mathbf{u} \in V$.

3. Polar spaces

When β is non-degenerate σ-sesquilinear form on $V(n,q)$, a vector $\mathbf{u}$ is *isotropic* if $\beta(\mathbf{u},\mathbf{u})=0$. A subspace U is *tatally isotropic* if $\beta(\mathbf{u},\mathbf{v})=0$ for all $\mathbf{u},\mathbf{v}\in U$. A pair $(\mathbf{u},\mathbf{v})$ of isotropic vectors is *hyperbolic pair* if $\beta(\mathbf{u},\mathbf{v})=1$. A subspace U is *anisotropic* if $\beta(\mathbf{u},\mathbf{u})\neq 0$ for all $\mathbf{u}\in U$.

Let Q be a non-singular quadratic form on $V(n,q)$. a vector $\mathbf{u}$ is *singular* if $Q(\mathbf{u})=0$. A subspace U is *tatally singular* if $Q(\mathbf{u})=0$ for all $\mathbf{v}\in U$. A pair $(\mathbf{u},\mathbf{v})$ of singular vectors is *hyperbolic pair* if $\beta(\mathbf{u},\mathbf{v})=1$. A subspace U is *anisotropic* if $Q(\mathbf{u})\neq 0$ for all $\mathbf{u}\in U$.

Polar space is a projective geometry whose points, lines, planes, ..., are totally isotropic or totally singular subspaces with σ-sesquilinear form or quadratic form.

If the form is alternating corresponding polar space is called *symplectic*, if hermitian then called *unitary*, if quadratic form then is called *orthogoal*.

LEMMA 3.1. [3] *Suppose that L is a subspace of rank 2 of $V(n,q)$ that contains a singular vector $\mathbf{u}$ with respect to a quadratic form Q. Either Q resricted to L is singular or there is a vector $\mathbf{u}$ such that $(\mathbf{u},\mathbf{v})$ is a hyperbolic pair and $L=\langle\mathbf{u},\mathbf{v}\rangle$.*

THEOREM 3.2. [3] *Let Q be a non-singular quadratic form on $V(n,q)$. Let W be a maximal totally isotropic subspace. Then there exists a basis $\{\mathbf{e}_i|\, i=1,2,\ldots,r\}\cup\{\mathbf{f}_i|\, i=1,2,\cdots,r\}$ for a subspace $X\leq V$ such that $V=X\oplus U$, where $(\mathbf{e}_i,\mathbf{f}_i)$ is a hyperbolic pair and U is a anisotropic.*

Note that in above theorem r is invariant given V and β, and is called *rank of a polar space*. We can easily deduce that $r\leq n/2$. In the followings notice that the notation r means polar rank.

LEMMA 3.3. [3] *Let Q be a non-singular quadratic form on $V(n,q)$. If the rank of V is at least 3 then V has an isotropic vector.*

By 3.3 the rank of anisotropic subspace U is to be $0,1,2$. Applying this theorem we now proceed the following.

THEOREM 3.4. [4] *Let Q be a non-singular quadratic form on $V(n,q)$. Then $n=2r$, $2r+1$, $2r+2$ and respectively, there is a basis B with respect to which*

$$Q(u)=u_1u_2+\cdots+u_{2r-1}u_{2r}\,,$$

$$Q(u) = u_1u_2 + \cdots + u_{2r-1}u_{2r} + au_{2r+1}^2\,,$$

where $a = 1$ if q is even and $a = 1$ or a chosen non-square if q is odd,

$$Q(u) = u_1u_2 + \cdots + u_{2r-1}u_{2r} + u_{2r+1}^2 + au_{2r+1}u_{2r+2} + bu_{2r+2}^2\,,$$

where $b = 1$ and the trace $Tr_\sigma(a^{-1})$ from $GF(q)$ to $GF(2)$ is 1 if q is even and $a = 0$ and $-b$ is a chosen non-square if q is odd.

In three cases if $n = 2r$ then quadratic form Q is called *hyperbolic* , if $n = 2r + 1$ then Q is called *parabolic* and if $n = 2r + 2$ then Q is called *elliptic*.

THEOREM 3.5. [2] *Let V be a finite geometry over $V(n, q)$ with an orthonormal basis. Let r be the rank of maximal self-orthogonal subspace. Then for n even, $n = 2r$ whenever $(-1)^{n/2}$ is square in $GF(q)$, and $n = 2r + 2$ whenever $(-1)^{n/2}$ is not square in $GF(q)$. In case n is odd, $n = 2r + 1$*

Thus we can know that if $n = 2r$ and $(-1)^{n/2}$ is square then quadratic form is hyperbolic, if $n = 2r$ and $(-1)^{n/2}$ is not square then quadratic form is elliptic and if $n = 2r + 1$ then quadratic form is parabolic.

THEOREM 3.6. *Self orthogonal code is orthogonal polar space*

Proof. Let $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n)$ in $V(n, q)$, and define $Q(\mathbf{u}) = u_1^2 + \ldots + u_n^2$. Clearly $Q(a\mathbf{u}) = a^2Q(\mathbf{u})$, $\beta(\mathbf{u}, \mathbf{v}) = Q(\mathbf{u} + \mathbf{v}) - Q(\mathbf{u}) - Q(\mathbf{v}) = 2u_1v_1 + \ldots 2u_nv_n$ is bilinear. These impliy that Q is quadratic form. Let C be a self orthogonal code. For all $\mathbf{u}, \mathbf{v} \in C$, we have $\mathbf{u} \cdot \mathbf{v} = 0$, so $\beta(\mathbf{u}, \mathbf{v}) = 2\mathbf{u} \cdot \mathbf{v} = 0$. It follows that $Q(\mathbf{u}) = 0$ for all $\mathbf{u} \in C$. □

4. Counting in polar spaces

The next theorem is well known.

THEOREM 4.1. *The number of subspaces of rank k in $V(n, q)$ is*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})},$$

Let U be a subspace of $V = V(n, q)$ with rank k. Then V/U is vector space and the rank is $n-k$. In addition V/U is isomorphic to $V(n-k, q)$. We want to apply similar argument to the followings. Suppose that P

is a polar space with rank r in V and let U be totally singular one dimensional subspace. Note that $U^{\perp} = \{\mathbf{v} \mid \beta(\mathbf{u}, \mathbf{v}) = 0 \text{ for all } \mathbf{u} \in U\}$. We define $Q_U(\mathbf{x} + U) = Q(\mathbf{x})$ in $U^{\perp}/U$. Then for $\mathbf{u} \in U$, $\mathbf{x} \in U^{\perp}$, $Q_U(\mathbf{x}+\mathbf{u}+U) = Q(\mathbf{x}+\mathbf{u}) = \beta(\mathbf{x}, \mathbf{u})+Q(\mathbf{x})+Q(\mathbf{u}) = Q(\mathbf{x}) = Q_U(\mathbf{x}+U)$. Therefore Q_U is well-defined quadratic form. So we can have next two theorems.

THEOREM 4.2. [4] *P is a polar space of rank r in $V(n, q)$ and U is totally singular 1-dimensional subspace. Then $U^{\perp}/U$ is a polar space of rank $r - 1$ of the same type as P.*

COROLLARY 4.3. *P is a polar space of rank r in $V(n, q)$ and U is totally singular k-dimensional subspace. Then $U^{\perp}/U$ is a polar space of rank $r - k$ of the same type as P.*

Proof. Suppose that $U = \langle e_1, \cdots e_k \rangle$ and $k \leq r$. By 3.2 we can choose a basis such that $V = \langle e_1, f_1, \cdots, e_k, f_k, \cdots e_r, f_r \rangle \oplus A$, where A is anisotropic subspace. Then $U^{\perp}/U = \langle e_{k+1}, f_{k+1}, \cdots e_r, f_r \rangle \oplus A$. □

We assign a fixed ϵ-value to each polar space as follows.

Form	n	Polar space	ϵ
Alternating	$2r$	Sympletic	0
Hermitian	$2r$	Unitary	$-\frac{1}{2}$
Hermitian	$2r+1$	Unitary	$\frac{1}{2}$
Quadratic	$2r$	Hyperbolic	-1
Quadratic	$2r+1$	Parabolic	0
Quadratic	$2r+2$	Elliptic	1

THEOREM 4.4. [3] *The number of points of a finite polar space P of rank r is*

$$\frac{(q^r - 1)(q^{r+\epsilon} + 1)}{q - 1}$$

THEOREM 4.5. [3] *The number of $(r-1)$-dimensional subspaces of a finite polar space P of a rank r is*

$$\prod_{i=1}^{r} \left(q^{i+\epsilon} + 1\right)$$

THEOREM 4.6. *The number of $(k-1)$-dimensional subspaces in polar space P of rank r is*

$$\prod_{i=r-k+1}^{r} \left(q^{i+\epsilon}+1\right) \cdot \begin{bmatrix} r \\ k \end{bmatrix}_q$$

Proof. Let $S(k)$ be the number of totally singular $(k-1)$-dimensional subspaces of a finite polar space P of a rank r. We just need to find the $S(k)$ to prove the theorem. Let $H(r)$ be the number of $r-1$ dimensional subspaces in a polar space of rank r. Assume U is a totally singular subspace with dimension $k-1$. Let's we count the number of pair (U, W), where W is a maximal totally singular subspace in V that containing U. By 4.3 $U/U^{\perp}$ is polar space of rank $r-k$. If W' is maximal singular space in $U/U^{\perp}$ then $W = \langle U, W' \rangle$ is maximal singular subspace in V. Hence if we count U first, the number of pairs is $S(k)H(r-k)$. If we count W first, the number of pairs is $H(r) \begin{bmatrix} r \\ k \end{bmatrix}_q$. We thus get following relation.

$$S(k)H(r-k) = H(r) \begin{bmatrix} r \\ k \end{bmatrix}_q$$

i.e,

$$S(k) \prod_{i=1}^{r-k} \left(q^{i+\epsilon}+1\right) = \prod_{i=1}^{r} \left(q^{i+\epsilon}+1\right) \begin{bmatrix} r \\ k \end{bmatrix}_q$$

implies

$$S(k) = \prod_{i=r-k+1}^{r} \left(q^{i+\epsilon}+1\right) \cdot \begin{bmatrix} r \\ k \end{bmatrix}_q$$

□

THEOREM 4.7. [1, 2] *Let $\sigma(n,k)$ be the number of self-orthogonal codes of length n and dimension k over $GF(q)$, where q is odd. Then:*

1. If n is odd,

$$\sigma(n,k) = \frac{\prod_{i=0}^{k-1}(q^{(n-1-2i)}-1)}{\prod_{i=1}^{k}(q^i-1)}.$$

2. If n is even and $(-1)^{n/2}$ is square

$$\sigma(n,k)=\frac{(q^{n-k}-q^{n/2-k}+q^{n/2}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{i=1}^{k}(q^i-1)},(k\geq 2)$$

3. If n is even and $(-1)^{n/2}$ is not square

$$\sigma(n,k)=\frac{(q^{n-k}+q^{n/2-k}-q^{n/2}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{i=1}^{k}(q^i-1)},(k\geq 2)$$

Proof. Suppose that n is odd, $n=2r+1$, r is polar rank. The notation $S(k)$ is same as previous theorem.

$$\begin{aligned}\sigma(n,k)=S(k)&=\prod_{i=r-k+1}^{r}\left(q^i+1\right)\begin{bmatrix}r\\k\end{bmatrix}_q\\&=(q^{r-k+1}+1)\cdots(q^r+1)\frac{(q^r-1)(q^r-q)\cdots(q^r-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}\\&=(q^{r-k+1}+1)\cdots(q^r+1)\frac{(q^r-1)(q^{r-1}-1)\cdots(q^{r-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}\\&=\frac{(q^{2r-2k+2}-1)\cdots(q^{2r}-1)}{(q^k-1)\cdots(q-1)}\\&=\frac{(q^{n-2k+1}-1)\cdots(q^{n-1}-1)}{(q^k-1)\cdots(q-1)}\\&=\frac{\prod_{i=0}^{k-1}(q^{n-1-2i}-1)}{\prod_{i=1}^{k}(q^i-1)}.\end{aligned}$$

Suppose that n is even and $n=2r$. In this case $\epsilon=-1$, So we get following.

$$\begin{aligned}
\sigma(n,k) = S(k) &= \prod_{i=r-k+1}^{r} \left(q^{i-1}+1\right) \begin{bmatrix} r \\ k \end{bmatrix}_q \\
&= (q^{r-k}+1)\cdots(q^{r-1}+1)\frac{(q^r-1)(q^r-q)\cdots(q^r-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} \\
&= (q^{r-k}+1)\cdots(q^{r-1}+1)\frac{(q^r-1)(q^{r-1}-1)\cdots(q^{r-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \\
&= \frac{(q^{r-k}+1)(q^r-1)(q^{2r-2}-1)\cdots(q^{2r-2k+2}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{2r-k}-q^{r-k}+q^r-1)(q^{2r-2}-1)\cdots(q^{2r-2k+2}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{n-k}-q^{n/2-k}+q^{n/2}-1)(q^{n-2}-1)\cdots(q^{n-2k+2}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{n-k}-q^{n/2-k}+q^{n/2}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{i=1}^{k}(q^i-1)}
\end{aligned}$$

Suppose that n is even and $n = 2r+2$. In this case $\epsilon = 1$, So we get following.

$$\begin{aligned}
\sigma(n,k) = S(k) &= \prod_{i=r-k+1}^{r} \left(q^{i+1}+1\right) \begin{bmatrix} r \\ k \end{bmatrix}_q \\
&= (q^{r-k+2}+1)\cdots(q^{r+1}+1)\frac{(q^r-1)(q^r-q)\cdots(q^r-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} \\
&= (q^{r-k+2}+1)\cdots(q^{r+1}+1)\frac{(q^r-1)(q^{r-1}-1)\cdots(q^{r-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \\
&= \frac{(q^{r+1}+1)(q^{r-k+1}-1)(q^{2r}-1)\cdots(q^{2r-2k+4}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{2r-k+2}-q^{r+1}+q^{r-k+1}-1)(q^{2r}-1)\cdots(q^{2r-2k+4}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{n-k}-q^{n/2}+q^{n/2-k}-1)(q^{n-2}-1)\cdots(q^{n-2k+2}-1)}{(q^k-1)\cdots(q-1)} \\
&= \frac{(q^{n-k}+q^{n/2-k}-q^{n/2}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{i=1}^{k}(q^i-1)}
\end{aligned}$$

□

In this mass formula when n is even, $\sigma(n,1)$ was omitted. One dimensional self orthogonal codes in $V(n,q)$ is corresponded to points in polar space. Thus by 4.4, $\sigma(n,1) = (q^r-1)(q^{r+\epsilon}+1)/(q-1)$. If $(-1)^{n/2}$ is square then $n = 2r$ and $\epsilon = -1$, so

$$\sigma(n,1) = \frac{q^{n-1} + q^{n/2} - q^{n/2-1} - 1}{q-1}$$

If $(-1)^{n/2}$ is not square then $n = 2r+2$ and $\epsilon = 1$, thus

$$\sigma(n,1) = \frac{q^{n-1} - q^{n/2} + q^{n/2-1} - 1}{q-1}$$

References

[1] V.S. Pless, *The number of isotropic subspace in a finite geometry*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei **39** (1965), 418–421.

[2] V.S. Pless, *On the uniqueness of the Golay codes*, J. Combin. Theory **5** (1968), 215–228.

[3] Simeon Ball and Zsuasa Weiner, *An Introduction to Finite Geometry* (2011).

[4] Simeon Ball *Finite Geometry and Combinatorial Applications*, Cambridge University Press (2015).

[5] R.A.L. Betty and A. Munemasa, *Mass formula for self-orthogonal codes over* Z_{p^2}, J.Combin.Inform.System sci.,

[6] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, *Mass formula for self-dual codes over* Z_{p^2}, Discrete Math. **308** (2008), 2984–3002 .

[7] Y.H. Park, *The classification of self-dual modular codes*, Finite Fields and Their Applications **17** (5) (2011), 442–460.

[8] W. Cary Huffman and Vera Pless, *Fundamentals of error correcting codes*, Cambridge University Pless, New York, 2003.

Kwang Ho Kim
Department of Mathematics
Kangwon National University
Chuncheon 24341, Korea
E-mail: prime229@gmail.com

Young Ho Park
Department of Mathematics
Kangwon National University
Chuncheon 24341, Korea
E-mail: yhpark@kangwon.ac.kr