A characteristic property of self-orthogonal codes and its application to lattices

Zhe-Xian Wan

Abstract

Let p be an odd prime, $\zeta = e^{2\pi i/p}$, D be the ring of algebraic integers in the field $Q(\zeta)$, and $P = (1-\zeta)$ be the principal ideal of D generated by $1-\zeta$. For a p-ary linear code C of length n, define the lattice $\Lambda_C = \{p^{-1/2}(\mathbf{c}+\mathbf{z}) \mid \mathbf{c} \in C,\ \mathbf{z} \in P^n\}$. It is proved that Λ_C is even if and only if C is self-orthogonal and that Λ_C is even unimodular if and only if C is self-dual. The proof rests on the following remark that for an odd prime power q a q-ary linear code C is self-orthogonal if and only if $\mathbf{c} \cdot \mathbf{c} = 0$ for all $\mathbf{c} \in C$. Finally, irreducible root lattices arising as Λ_C from p-ary linear codes C are completely determined.

1 Introduction

Let q be a prime power, n be a positive integer, and $\mathbb{F}_q^n$ be the n-dimensional row vector space over the finite field $\mathbb{F}_q$ with q elements. A k-dimensional subspace of $\mathbb{F}_q^n$ is called a q-ary linear $[n,k]$-code. For any $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, define

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n.$$

Let C be a q-ary linear $[n,k]$-code. Define

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \ \text{ for all } \ \mathbf{y} \in C\}.$$

Then $C^\perp$ is an $(n-k)$-dimensional subspace of $\mathbb{F}_q^n$ and called the *dual code* of C. If $C \subseteq C^\perp$, then C is called *self-orthogonal*. If $C = C^\perp$, then C is called *self-dual*.

Received by the editors August 1997.
Communicated by James Hirschfeld.
1991 *Mathematics Subject Classification.* 05, 94.
Key words and phrases. self-orthogonal code, cyclotomic field, lattice, irreducible root lattice.

In the present paper it is remarked that when q is a power of an odd prime, a q-ary linear code C is self-orthogonal if and only if $\mathbf{c}\cdot\mathbf{c}=0$ for all $\mathbf{c}\in C$. Then this remark is applied to the study of lattices.

Let p be an odd prime, $\zeta=e^{2\pi i/p}, \mathbb{Q}(\zeta)$ be the cyclotomic field of pth roots of unity, D be its ring of algebraic integers, and $P=(1-\zeta)$ be the principal ideal of D generated by $1-\zeta$.

For a p-ary linear $[n,k]$-code C, define the lattice

$$\Lambda_C=\{p^{-1/2}(\mathbf{c}+\mathbf{z}) \mid \mathbf{c}\in C,\ \mathbf{z}\in P^n\},$$

where $\mathbf{c}$ is regarded as a vector whose components are integers $0,1,\dots,p-1$. Then it is proved that Λ_C is even if and only if C is self-orthogonal and that Λ_C is even unimodular if and only if C is self-dual. This improves a proposition of [1].

Finally, let Λ be an irreducible root lattice in $\mathbb{R}^n$. Then it is proved that $\Lambda\simeq\Lambda_C$ for a p-ary code C of length n, where p is an odd prime, if and only if Λ is of type A_{p-1}, E_6 (when $p=3$ and $n=3$), or E_8 (when $p=3$ and $n=4$, or $p=5$ and $n=2$).

2 A characteristic property of self-orthogonal codes

Proposition 1
Let q be a power of an odd prime and C be a q-ary linear code. Then C is self-orthogonal if and only if $\mathbf{c}\cdot\mathbf{c}=0$ for all $\mathbf{c}\in C$.

Proof. Assume that $\mathbf{c}\cdot\mathbf{c}=0$ for all $\mathbf{c}\in C$. For any $\mathbf{c}$, $\mathbf{c}'\in C$, since C is linear, $\mathbf{c}+\mathbf{c}'\in C$. Then

$$\mathbf{c}\cdot\mathbf{c}=\mathbf{c}'\cdot\mathbf{c}'=(\mathbf{c}+\mathbf{c}')\cdot(\mathbf{c}+\mathbf{c}')=0,$$

which implies $2\mathbf{c}\cdot\mathbf{c}'=0$. Since q is odd, we have $\mathbf{c}\cdot\mathbf{c}'=0$ for all $\mathbf{c},\mathbf{c}'\in C$. Therefore $C\subseteq C^{\perp}$.

The converse part is trivial. ■

Proposition 1 should be known, but the author could not find a reference, so let its proof be here.

The following example shows that Proposition 1 does not always hold when q is even.

Example

Let

$$C=\{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}\subseteq\mathbb{F}_2^3.$$

Clearly, C is a binary linear $[3,2]$-code with the property that $\mathbf{c}\cdot\mathbf{c}=0$ for all $\mathbf{c}\in C$, but $C\not\subseteq C^{\perp}$.

For the following proposition, see, for example, [1], p. 9 or [4], p. 26.

Proposition 2
Let q be a prime power and C be a q-ary linear $[n,k]$-code. Then C is self-dual if and only if n is even, $k=n/2$, and $C\subseteq C^{\perp}$.

3 Application to lattices

Let p be an odd prime, $\zeta = e^{2\pi i/p}$, $\mathbb{Q}(\zeta)$ be the cyclotomic field of pth roots of unity, and D be its ring of algebraic integers. It may be shown (see, for example, [3], Chapter 13, §2) that

$$\begin{aligned}\mathbb{Q}(\zeta) &= \mathbb{Q} + \mathbb{Q}\zeta + \cdots + \mathbb{Q}\zeta^{p-2},\\ D &= \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2},\end{aligned}$$

where both sums are direct. Also the ideal $P = (1-\zeta)$ is a prime ideal of D, $\bar{P} = P$, and $D/P \simeq \mathbb{F}_p$. Define a bilinear form on $\mathbb{Q}(\zeta)$ by

$$(x, y) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x\bar{y}) \ \text{ for all } \ x, y \in \mathbb{Q}(\zeta),$$

where $\bar{y}$ denotes the complex conjugate of y. It was proved (see, for example, [1], §5.1 or [2]) that it is a positive definite symmetric bilinear form on $\mathbb{Q}(\zeta)$, that D is a $(p-1)$-dimensional lattice with disc $D = p^{p-2}$, and that $p^{-1/2}P$ is a $(p-1)$-dimensional lattice of type A_{p-1}.

Let n be an integer ≥ 2,

$$\mathbb{Q}(\zeta)^n = \{\mathbf{x} = (x_1, \ldots, x_n) \mid x_i \in \mathbb{Q}(\zeta)\}$$

and define

$$(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} (x_i, y_i) \ \text{ for all } \ \mathbf{x}, \mathbf{y} \in \mathbb{Q}(\zeta).$$

Then $(\mathbf{x}, \mathbf{y})$ is a positive definite symmetric bilinear form on $\mathbb{Q}(\zeta)^n$. Moreover, D^n is an $n(p-1)$-dimensional lattice with disc $D^n = p^{n(p-2)}$, and $p^{-1/2}P^n$ is an $n(p-1)$-dimensional lattice of type nA_{p-1}.

Define a map $\rho : D^n \to (D/P)^n \simeq \mathbb{F}_p^n$ by

$$\rho(x_1, \ldots, x_n) = (x_1 + P, \ldots, x_n + P) \ \text{ for all } \ (x_1, \ldots, x_n) \in D^n.$$

Clearly, ρ is a surjective homomorphism of additive groups. Let C be a p-ary linear $[n, k]$-code. Define

$$\begin{aligned}\Lambda_C &= p^{-1/2}\rho^{-1}(C)\\ &= \{p^{-1/2}(\mathbf{c} + \mathbf{z}) \mid \mathbf{c} \in C, \ \mathbf{z} \in P^n\},\end{aligned}$$

where $\mathbf{c}$ is regarded as a vector whose components are integers $0, 1, \ldots, p-1$. Then we have

Proposition 3
Let p be an odd prime and C be a p-ary linear $[n, k]$-code. Then Λ_C is an $n(p-1)$-dimensional lattice containing the lattice $p^{-1/2}P^n$ of type nA_{p-1} and with disc $\Lambda_C = p^{n-2k}$. Moreover,

(i) Λ_C is even if and only if C is self-orthogonal.
(ii) Λ_C is even unimodular if and only if C is self-dual.

Proof. We have $|\ \mathbb{F}_p^n/C\ | = p^{n-k}$. By the 2nd isomorphism theorem (see [5], p. 150)

$$D^n/\rho^{-1}(C) \simeq \mathbb{F}_p^n/C.$$

Therefore $|\ D^n/\rho^{-1}(C)\ | = p^{n-k}$. Since D^n is an $n(p-1)$-dimensional lattice, so is $\rho^{-1}(C)$. It follows that $\Lambda_C = p^{-1/2}\rho^{-1}(C)$ is also an $n(p-1)$-dimensional lattice. We have

$$\begin{aligned} \operatorname{disc}\Lambda_C &= ((p^{-1/2})^{n(p-1)})^2 \ \operatorname{disc}\rho^{-1}(C) \\ &= p^{-n(p-1)} \ \operatorname{disc} D^n \ |\ D^n/\rho^{-1}(C)\ |^2 \\ &= p^{-n(p-1)} p^{n(p-2)} p^{2(n-k)} \\ &= p^{n-2k}. \end{aligned} \tag{1}$$

(i) For any $\mathbf{x} \in \Lambda_C$, $\mathbf{x}$ can be expressed as

$$\mathbf{x} = p^{-1/2}(\mathbf{c} + \mathbf{z}), \quad \text{where } \ \mathbf{c} \in C, \ \mathbf{z} \in P^n.$$

Then

$$(\mathbf{x}, \mathbf{x}) = p^{-1}\left(\operatorname{Tr}(\mathbf{c}\cdot\mathbf{c}) + \operatorname{Tr}(\mathbf{c}(\mathbf{z} + \bar{\mathbf{z}})) + \operatorname{Tr}(\mathbf{z}\bar{\mathbf{z}})\right),$$

where $\operatorname{Tr} = \operatorname{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$. It is easy to verify that

$$\operatorname{Tr}(\mathbf{c}\cdot\mathbf{c}) = (p-1)(\mathbf{c}\cdot\mathbf{c})$$

and

$$\operatorname{Tr}(y + \bar{y}), \operatorname{Tr}(y\bar{y}) \in 2p\mathbb{Z} \ \text{ for all } \ y \in P.$$

Thus,

$$\begin{aligned} (\mathbf{x}, \mathbf{x}) &= p^{-1}((p-1)(\mathbf{c}\cdot\mathbf{c}) + 2pr), \quad \text{where } \ r \in \mathbb{Z} \\ &= p^{-1}(p-1)(\mathbf{c}\cdot\mathbf{c}) + 2r. \end{aligned}$$

Therefore,

$$\begin{aligned} (\mathbf{x}, \mathbf{x}) \in 2\mathbb{Z} &\Leftrightarrow \ p \mid \mathbf{c}\cdot\mathbf{c} \\ &\Leftrightarrow \ \mathbf{c}\cdot\mathbf{c} = 0 \ \text{ in } \ \mathbb{F}_p. \end{aligned}$$

Hence, Λ_C is even if and only if $\mathbf{c}\cdot\mathbf{c} = 0$ for all $\mathbf{c} \in C$. By Proposition 1, Λ_C is even if and only if C is self-orthogonal.

(ii) By (1), $\operatorname{disc}\Lambda_C = 1$ if and only if $n = 2k$, i.e., n is even and $k = n/2$. By Proposition 2 and (i),

$$\begin{aligned} C \text{ is self-dual} &\Leftrightarrow \ n \text{ is even, } k = n/2, \text{ and } C \subseteq C^{\perp} \\ &\Leftrightarrow \ \operatorname{disc}\Lambda_C = 1 \text{ and } \Lambda_C \text{ is even} \\ &\Leftrightarrow \ \Lambda_C \text{ is even unimodular.} \end{aligned}$$

■

The "if" parts of Proposition 3 can be found in [1], i.e., Proposition 5.2 of [1], p. 135.

Let Λ be a lattice in $\mathbb{R}^n$. Define

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z} \text{ for all } \mathbf{y} \in \Lambda\}.$$

Then Λ^* is also a lattice in $\mathbb{R}^n$, called the *dual lattice* of Λ. Λ is called *integral* if $\mathbf{x} \cdot \mathbf{y} \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \Lambda$. For an integral lattice Λ, $\Lambda \subseteq \Lambda^*$ and Λ^*/Λ is a finite abelian group. Λ is called *even* if $\mathbf{x} \cdot \mathbf{x} \in 2\mathbb{Z}$ for all $\mathbf{x} \in \Lambda$. If Λ is even then it is integral.

Let Λ be an even lattice. A vector of square length 2 in Λ is called a *root* of Λ. If Λ is generated by all its roots, Λ is called a *root lattice*. If Λ cannot be written as the direct sum of two sublattices Λ_1 and Λ_2 such that $(\mathbf{x}_1, \mathbf{x}_2) = 0$ for all $\mathbf{x}_1 \in \Lambda_1$ and $\mathbf{x}_2 \in \Lambda_2$, Λ is called *irreducible*. It is known that irreducible root lattices are of types $A_n (n \geq 1)$, D_n (n even and ≥ 4), $E_n (n = 6, 7, 8)$, (cf. Theorem 1.2 of [1], p. 20). If irreducible root lattices Λ and Λ' are of the same type, we write $\Lambda \simeq \Lambda'$.

As in the binary case we can study which irreducible root lattices arise as lattices Λ_C from p-ary codes C.

Lemma 1
Let C be a p-ary linear code, then $\Lambda_C^* = \Lambda_{C^\perp}$.

Proof. Let $\mathbf{x} = p^{-1/2}(\mathbf{c} + \mathbf{z}) \in \Lambda_C$ and $\mathbf{y} = p^{-1/2}(\mathbf{c}' + \mathbf{z}') \in \Lambda_{C^\perp}$, where $\mathbf{c} \in C$, $\mathbf{c}' \in C^\perp$, and $\mathbf{z}, \mathbf{z}' \in P^n$. Then

$$(\mathbf{x}, \mathbf{y}) = p^{-1} \ \mathrm{Tr}(\mathbf{c} \cdot \mathbf{c}' + \mathbf{c} \cdot \overline{\mathbf{z}'} + \mathbf{z} \cdot \mathbf{c}' + \mathbf{z} \cdot \overline{\mathbf{z}'}).$$

For $\mathbf{c} \in C$ and $\mathbf{c}' \in C^\perp$ we have $\mathbf{c} \cdot \mathbf{c}' = 0$ in $\mathbb{F}_p$. Computed in $\mathbb{C}$, $\mathbf{c} \cdot \mathbf{c}' \equiv 0 \pmod p$. Since $\mathbf{z}, \mathbf{z}' \in P^n$ and $\overline{P^n} = P^n$, we have $\mathbf{c} \cdot \overline{\mathbf{z}'}, \mathbf{z} \cdot \mathbf{c}', \mathbf{z} \cdot \overline{\mathbf{z}'} \in P$. Thus $\mathrm{Tr}(\mathbf{c} \cdot \mathbf{c}' + \mathbf{c} \cdot \overline{\mathbf{z}'} + \mathbf{z} \cdot \mathbf{c}' + \mathbf{z} \cdot \overline{\mathbf{z}'}) \in p\mathbb{Z}$. Therefore $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}$. This proves $\Lambda_{C^\perp} \subseteq \Lambda_C^*$.

Let $\dim C = k$. By Proposition 3, disc $\Lambda_C = p^{n-2k}$ and disc $\Lambda_{C^\perp} = p^{2k-n}$. But disc $\Lambda_C^* = (\text{disc } \Lambda_C)^{-1} = p^{2k-n}$. Therefore disc $\Lambda_{C^\perp} =$ disc Λ_C^*. Hence $\Lambda_{C^\perp} = \Lambda_C^*$. ■

Proposition 4
Let Λ be an irreducible root lattice in $\mathbb{R}^n$. Then $\Lambda \simeq \Lambda_C$ for a p-ary linear code C of length n, where p is an odd prime if and only if Λ is of type A_{p-1}, E_6 (when $p = 3$ and $n = 3$), or E_8 (when $p = 3$ and $n = 4$, or $p = 5$ and $n = 2$).

Proof. Assume that $\Lambda \simeq \Lambda_C$ for a p-ary linear code C of length n, where p is an odd prime. For any p-ary linear code C' of length n, let $\mathbf{x} \in L_{C'}$, then $\mathbf{x} = p^{-1/2}(\mathbf{c}' + \mathbf{z})$, where $\mathbf{c}' \in C$ and $\mathbf{z} \in P^n$. Thus $p\mathbf{x} = p^{-1/2}(p(\mathbf{c}' + \mathbf{z}))$ and $p(\mathbf{c}' + \mathbf{z}) \in P^n$. Therefore $p\Lambda_{C'} \subseteq p^{-1/2}P^n \subseteq \Lambda_C$. Since $\Lambda_C^* = \Lambda_{C^\perp}$, we have, in particular, $p\Lambda_C^* \subseteq \Lambda_C$. But Λ_C^*/Λ_C is a finite abelian group. So

$$\Lambda_C^*/\Lambda_C \simeq (\mathbb{Z}/p\mathbb{Z})^\ell \text{ for some } \ell \geq 0. \tag{2}$$

By inspecting the irreducible root lattices one by one we find that only A_{p-1}, E_6 (when $p = 3$), and E_8 satisfy the condition (2). Moreover, if $E_6 \simeq \Lambda_C$ for a p-ary linear code C of length n, then $6 = (p-1)n$, which implies $p = 3$ and $n = 3$. If $E_8 \simeq \Lambda_C$ for a p-ary linear code C of length n, then $8 = (p-1)n$. It follows that

$p = 3$ and $n = 4$ or $p = 5$ and $n = 2$. Therefore Λ is of type A_{p-1}, E_6 (when $p = 3$ and $n = 3$), or E_8 (when $p = 3$ and $n = 4$, or $p = 5$ and $n = 2$).

Conversely, assume that Λ is of type A_{p-1}, E_6, or E_8. If Λ is of type A_{p-1}, let C be the 1-dimensional code $\{0\}$ consisting of 0 only; then $\Lambda_C = p^{-1/2}P$, which is of type A_{p-1}. If Λ is of type E_6, let $C = \mathbb{F}_3(1, 1, 1)$; then $\Lambda \simeq \Lambda_C$. If Λ is of type E_8, let $C = \mathbb{F}_3(1, 0, 1, 1) + \mathbb{F}_3(0, 1, 1, 2)$ or $\mathbb{F}_5(1, 2)$; then $\Lambda \simeq \Lambda_C$. ■

References

[1] W. Ebeling. *Lattices and Codes.* Vieweg, Wiesbaden, 1994.

[2] F. Hirzebruch. A letter to N. J. A. Sloane on 19 August, 1986. In *Gesammelte Abhandlungen, Collected Papers*, pages 796–798. Band II. Springer, Berlin, 1987.

[3] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, New York, 2nd edition, 1990.

[4] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[5] B. L. van der Waerden. *Algebra I.* Springer, Berlin, 6 Auflage, 1964.

Zhe-Xian Wan
Department of Information Technology
Lund University
P.O. Box 118
S-221 00 Lund
Sweden
email: wan@it.lth.se