Note on Jacobi polynomials of binary codes

Nur Hamid[*], Tsuyoshi Miezaki[†] and Manabu Oura[‡]

Abstract

We investigate the Jacobi polynomials of binary codes in genus 1 and give the generators of a ring which is related to the Jacobi polynomials.

1 Introduction

The Jacobi polynomial is contained in the invariant ring of a group related to the binary codes. Under this relation, we show that the invariant ring for a group given can be generated by the Jacobi polynomials of the binary codes. We refer to [2] for the basic theory of Jacobi polynomial. The reader can see [1] for the generalization of Jacobi polynomial for the binary case.

Let $\mathbb{F}_2 = \{0, 1\}$. A code C of length n here means a linear subspace of $\mathbb{F}_2^n$. For $x, y \in \mathbb{F}_2^n$, the inner product $x \cdot y$ is defined by

$$x \cdot y := x_1 y_1 + \cdots + x_n y_n \in \mathbb{F}_2$$

and we denote by $x * y$ the number of the indices is such that $x_i \neq 0$ and $y_i \neq 0$.

For $c = (c_1, ..., c_n) \in C$, the weight $wt(c)$ is the number of nonzero c_i. The dual $C^\perp$ of C is defined by the set containing all $x \in \mathbb{F}_2^n$ such that

$$x \cdot y = 0$$

for all $y \in C$. The code C is called *Type II* if it satisfies the following conditions.

1. C is self-dual, that is $C = C^\perp$.

2. The weight $wt(c)$ of c is the multiple of 4 for all $c \in C$.

In this paper, the code used is d_n^+ whose generator matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & & & & \ddots & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & \dots & 1 & 0 & 1 & 0 \end{pmatrix}.$$

We close this section by giving the definition and the example of Jacobi polynomial.

[*](1) Graduate School of Natural Science and Technology, Kanazawa University, Japan, (2) Universitas Nurul Jadid, Paiton, Probolinggo, Indonesia

[†]Faculty of Education, University of the Ryukyus, Okinawa 903–0213, Japan miezaki@edu.u-ryukyu.ac.jp

[‡]Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa 920–1192, Japan oura@se.kanazawa-u.ac.jp

Definition 1.1. The Jacobi polynomial $Jac(C, v)$ of the code C with the reference vector v is defined by

$$Jac(C, v|x, y, z, w) := \sum_{u \in C} x^{n-wt(v)-wt(u)+u*v} y^{wt(u)-u*v} z^{wt(v)-u*v} w^{u*v}.$$

Example 1.1. Let $C = d_8^+$ and $v = (1, 0, 0, 0, 0, 0, 0, 0)$. The Jacobi polynomial of C with the reference vector v is

$$Jac(C, v) = x^7 w + 7x^3 y^4 w + 7x^4 y^3 z + y^7 z.$$

2 Results

Let G be a group generated by the matrices

$$\frac{\eta}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}, \begin{pmatrix} \eta & 0 & 0 & 0 \\ 0 & \eta & 0 & 0 \\ 0 & 0 & \eta & 0 \\ 0 & 0 & 0 & \eta \end{pmatrix}$$

where η is the 8-th primitive root of 1. The group G is of order 192.

We denote by $\mathfrak{R}$ the invariant ring of G:

$$\mathbb{C}[x, y, z, w]^G.$$

The dimension formula of $\mathfrak{R}$ is

$$\sum_n (\dim \mathfrak{R}) t^n = \frac{1 + 8t^8 + 21t^{16} + 58t^{24} + 47t^{32} + 35t^{40} + 21t^{48} + t^{56}}{(1 - t^8)^2 (1 - t^{24})^2}.$$

From the dimension formula of $\mathfrak{R}$, we have the following proposition.

Proposition 2.1. *The invariant ring $\mathfrak{R}$ can be generated by the Jacobi polynomials of binary codes of length 8, 16, 24, 32, 40, 48, 56 with at most 10, 21, 60, 47, 35, 21, 1 reference vectors, respectively.*

Using the Jacobi polynomials of the binary codes of length 8 and 24, we have the following result.

Theorem 2.1. *The ring $\mathfrak{R}$ can be generated by 10 Jacobi polynomials of the binary codes of length 8 and 25 Jacobi polynomials of binary codes of length 24.*

References

[1] Honma, K.; Okabe, T.; Oura, M.; Weight enumerators, intersection enumerators, and Jacobi polynomials. Discrete Math. 343 (2020), no. 6, 111815.

[2] Ozeki, M. On the notion of Jacobi polynomials for codes. Math. Proc. Cambridge. Philos. Soc. 121 (1997), no. 1, 15-30.

[3] SageMath, the Sage Mathematics Software System (Version 8.1), The Sage Developers, 2017, https://www.sagemath.org.