Discrete Mathematics 309 (2009) 570–575

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the dimensions of the binary codes of a class of unitals

Ka Hin Leung [a], Qing Xiang [b,*]

[a] Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Singapore

[b] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, United States

ARTICLE INFO

Article history:
Received 14 December 2006
Accepted 6 August 2008
Available online 10 September 2008

Keywords:
Buekenhout-Metz unital
Code
Design
Hermitian unital
Ideal
Unital

ABSTRACT

Let U_β be the special Buekenhout-Metz unital in PG$(2, q^2)$, formed by a union of q conics, where $q = p^e$ is an odd prime power. It can be shown that the dimension of the binary code of the corresponding unital design $\mathcal{U}_\beta$ is less than or equal to $q^3 + 1 - q$. Baker and Wantz conjectured that equality holds. We prove that the aforementioned dimension is greater than or equal to $q^3(1 - \frac{1}{p}) + \frac{q^2}{p}$.

1. Introduction

A *unital* is a 2-$(m^3 + 1, m + 1, 1)$ design, where $m \geq 2$. All known unitals with parameters $(m^3 + 1, m + 1, 1)$ have m equal to a prime power, except for one example with $m = 6$ constructed by Mathon [9], and independently by Bagchi and Bagchi [3]. In this note, we will only consider unitals embedded in PG$(2, q^2)$, i.e., unitals coming from a set of $q^3 + 1$ points of PG$(2, q^2)$ which meets every line of PG$(2, q^2)$ in either 1 or $q + 1$ points. (Sometimes, a point set of size $q^3 + 1$ of PG$(2, q^2)$ with the above line intersection properties is called a unital, too.) A classical example of such unitals is *the Hermitian unital* $\mathcal{U} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ and $\mathcal{B}$ are the set of absolute points and the set of non-absolute lines of a unitary polarity of PG$(2, q^2)$, respectively.

The Hermitian unital is a special example of a large class of unitals embedded in PG$(2, q^2)$, called the *Buekenhout-Metz unitals*. We refer the reader to [5] for a survey of results on these unitals. A subclass of the Buekenhout-Metz unitals which received some attention can be defined as follows.

Let $q = p^e$ be an **odd** prime power, where $e \geq 1$, let β be a primitive element of $\mathbb{F}_{q^2}$, and for $r \in \mathbb{F}_q$ let $C_r = \{(1, y, \beta y^2 + r) \mid y \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 1)\}$. We define

$$U_\beta = \bigcup_{r \in \mathbb{F}_q} C_r.$$

Note that each C_r is a conic in PG$(2, q^2)$, and any two distinct C_r have only the point $P_\infty = (0, 0, 1)$ in common. Hence $|U_\beta| = q^3 + 1$. It can be shown that every line of PG$(2, q^2)$ meets U_β in either 1 or $q + 1$ points (see [1,7]). One immediately obtains a unital (design) $\mathcal{U}_\beta$ from U_β: The *points* of $\mathcal{U}_\beta$ are the points of U_β, and the *blocks* of $\mathcal{U}_\beta$ are the intersections of the secant lines with U_β. In this note, we are interested in the binary code $\mathcal{C}_2(\mathcal{U}_\beta)$ of this design, i.e., the $\mathbb{F}_2$-subspace spanned by the characteristic vectors of the blocks of $\mathcal{U}_\beta$ in $\mathbb{F}_2^{U_\beta}$.

* Corresponding author.
E-mail addresses: matlkh@nus.edu.sg (K.H. Leung), xiang@math.udel.edu (Q. Xiang).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.08.004

The following proposition and its proof are due to Baker and Wantz [6,10]. To state the proposition, we use v^S to denote the characteristic vector of a subset S in U_β.

Proposition 1.1 (*Baker and Wantz*). *The vectors v^{C_r}, $r \in \mathbb{F}_q$, form a linearly independent set of vectors in $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$.*

Proof. A binary vector v lies in $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$, if and only if, each block of the design $\mathcal{U}_\beta$ meets the support of v in an even number of points. If a block of $\mathcal{U}_\beta$ goes through P_∞, then it meets every C_r in two points; if a block of $\mathcal{U}_\beta$ does not go through P_∞, then it meets every C_r in either 0 or 2 points. Hence $v^{C_r} \in \mathcal{C}_2(\mathcal{U}_\beta)^\perp$, for every $r \in \mathbb{F}_q$. The q conics C_r have only the point P_∞ in common. Thus, v^{C_r}, $r \in \mathbb{F}_q$, are linearly independent. The proof is complete. □

An immediate corollary of Proposition 1.1 is that $\dim\mathcal{C}_2(\mathcal{U}_\beta)^\perp \geq q$. Hence $\dim\mathcal{C}_2(\mathcal{U}_\beta) \leq q^3 + 1 - q$. Baker and Wantz [6,10] made the following conjecture.

Conjecture 1.2 (*Baker and Wantz*). *The 2-rank of $\mathcal{U}_\beta$ is $q^3 + 1 - q$. That is,* $\dim\mathcal{C}_2(\mathcal{U}_\beta) = q^3 + 1 - q$.

Wantz [10] verified Conjecture 1.2 in the cases where $q = 3, 5, 7$, and 9 by using a computer and MAGMA [4]. Gary Ebert [6] popularized the above conjecture of Baker and Wantz in a talk in Oberwolfach in 2001. See also [11] for a description of the above conjecture. Of course, the conjecture is equivalent to saying that $\dim \mathcal{C}_2(\mathcal{U}_\beta)^\perp = q$. So it suffices to show that $\{v^{C_r} \mid r \in \mathbb{F}_q\}$ spans $\mathcal{C}_2(\mathcal{U}_\beta)^\perp$. That is, we need to show that if $S \subset U_\beta$ and S meets every block of $\mathcal{U}_\beta$ in an even number of points, then S is a union of some C_r's, or a union of some C_r's with P_∞ deleted. We have not been able to prove this equivalent version of the conjecture. What we could prove is a lower bound on $\dim \mathcal{C}_2(\mathcal{U}_\beta)$ as stated in the abstract. The main idea in our proofs is to realize a shortened code of $\mathcal{C}_2(\mathcal{U}_\beta)$ as an ideal in a certain group algebra of the elementary abelian p-group of order q^3. We hope that the current note will stimulate further research on this conjecture.

2. A lower bound on the dimension of $\mathcal{C}_2(\mathcal{U}_\beta)$

We first consider the automorphisms of $\mathcal{U}_\beta$. Let

$$G = \{\theta \in \mathrm{PGL}(3, q^2) \mid \theta(U_\beta) = U_\beta\}$$

be the linear collineation group of $\mathrm{PG}(2, q^2)$ fixing U_β as a set. It was shown by Baker and Ebert [2] that

$$G = T \rtimes \mathbb{Z}_{2(q-1)},$$

where T is an elementary abelian group of order q^3, and $\mathbb{Z}_{2(q-1)}$ is a cyclic group of order $2(q-1)$. The group G certainly is also an automorphism group of the design $\mathcal{U}_\beta$ since any element of G maps a secant line of U_β to a secant line of U_β. In fact, the group T above acts regularly on $U_\beta \setminus \{P_\infty\}$. Explicitly,

$$T = \left\{ \begin{pmatrix} 1 & t & \beta t^2 \\ 0 & 1 & 2\beta t \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, t \in \mathbb{F}_{q^2}, r \in \mathbb{F}_q \right\} \cong (\mathbb{F}_{q^2}, +) \times (\mathbb{F}_q, +).$$

In the rest of the paper, we will use $T(t, r)$, $t \in \mathbb{F}_{q^2}$, $r \in \mathbb{F}_q$, to denote the element

$$\begin{pmatrix} 1 & t & \beta t^2 \\ 0 & 1 & 2\beta t \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

of T.

The coordinates of the code $\mathcal{C}_2(\mathcal{U}_\beta)$ are labeled by the points in U_β. Deleting the coordinate labeled by P_∞ from all codewords of $\mathcal{C}_2(\mathcal{U}_\beta)$, we get a shortened (or punctured) code $\mathcal{C}_2(\mathcal{U}_\beta)'$, which has the same dimension over $\mathbb{F}_2$ as $\mathcal{C}_2(\mathcal{U}_\beta)$ since $v^{\{P_\infty\}} \notin \mathcal{C}_2(\mathcal{U}_\beta)$. Since T acts regularly on $U_\beta \setminus \{P_\infty\}$, we may identify the coordinates of $\mathcal{C}_2(\mathcal{U}_\beta)'$ with the elements of T. Under this identification, the point $(1, t, \beta t^2 + r)$ of U_β correspond to the group element $T(t, r)$ since

$$(1, 0, 0) \cdot T(t, r) = (1, t, \beta t^2 + r).$$

After the above identification, the code $\mathcal{C}_2(\mathcal{U}_\beta)'$ becomes an ideal of the group algebra $\mathbb{F}_2[T]$. Now we can use the characters of T to help compute the dimension of $\mathcal{C}_2(\mathcal{U}_\beta)'$.

First of all, we need to extend the field over which the code $\mathcal{C}_2(\mathcal{U}_\beta)$ is defined. Let $K = \mathbb{F}_{2^m}$, where $m = \mathrm{ord}_p(2)$ is the order of 2 modulo p (i.e., m is the smallest positive integer such that $2^m \equiv 1 \pmod p$). So K contains a primitive pth root of unity ξ_p. We consider the code $\mathcal{C}_K(\mathcal{U}_\beta)$ and puncture it at P_∞ to get $\mathcal{C}_K(\mathcal{U}_\beta)'$, which will be denoted by M for simplicity of notation. The code M is an ideal of the group algebra $K[T]$, and

$$\dim_K(M) = \dim_{\mathbb{F}_2}(\mathcal{C}_2(\mathcal{U}_\beta)').$$