Good self-dual quasi-cyclic codes exist

Ling, San; Sole, Patrick

2003

Ling, S., & Solé, P. (2003). Good self-dual quasi-cyclic codes exist. IEEE Transactions on Information Theory, 49(4), 1052-1053.

https://hdl.handle.net/10356/96309

https://doi.org/10.1109/TIT.2003.809501

Good Self-Dual Quasi-Cyclic Codes Exist

San Ling and Patrick Solé, *Member, IEEE*

***Abstract*—We show that there are long binary quasi-cyclic self-dual (either Type I or Type II) codes satisfying the Gilbert–Varshamov bound.**

***Index Terms*—Cubing construction, Gilbert–Varshamov bound, quasi-cyclic codes, self-dual codes.**

I. Introduction

It has been known for 30 years that good long self-dual codes exist [6], and for more than a quarter century [1] that there are good long quasi-cyclic codes of rate $1/2$.

In this correspondence, we show that good long self-dual quasi-cyclic codes exist. Building on well-known mass formulas for self-dual binary and quaternary codes, we derive a Gilbert–Varshamov bound for long binary self-dual quasi-cyclic codes.

The proof uses the cubing construction of [5], [3] and the proof technique of [6].

As suggested by one referee, it might have been possible to build on [1] to derive this asymptotic result. However, [1] uses quasi-cyclic codes of index 2 while we use quasi-cyclic codes of index $n/3$, where n denotes the length. In some sense, we provide information on a different asymptotic ensemble of codes than [1].

II. Known Facts and Notations

A code is said to be **quasi-cyclic** of **index** ℓ or ℓ-quasi-cyclic if and only if it is invariant under T^ℓ, where T denotes the cyclic shift. If $\ell = 1$, such a code is just a cyclic code. We assume that all binary codes are equipped with the Euclidean inner product and all the $\boldsymbol{F}_4$-codes are equipped with the Hermitian inner product. The latter condition is necessary, when using the cubing construction, to ensure that the resulting binary code is Euclidean self-dual. Self-duality in the following discussion is with respect to these respective inner products. A binary self-dual code is said to be of Type II if and only if all its weights are multiples of 4 and of Type I otherwise. We first recall some background material on mass formulas for self-dual binary and quaternary codes.

Proposition 2.1: Let ℓ be an even positive integer.

i) The number of self-dual binary codes of length ℓ is given by

$$N(2, \ell) = \prod_{i=1}^{\frac{\ell}{2}-1} (2^i + 1).$$

ii) Let $\boldsymbol{v}$ be a codeword of length ℓ and even Hamming weight, other than $\boldsymbol{0}$ and $\boldsymbol{1}$. The number of self-dual binary codes of length ℓ containing $\boldsymbol{v}$ is given by

$$M(2, \ell) = \prod_{i=1}^{\frac{\ell}{2}-2} (2^i + 1).$$

iii) The number of self-dual $\boldsymbol{F}_4$-codes of length ℓ is given by

$$N(4, \ell) = \prod_{i=0}^{\frac{\ell}{2}-1} (2^{2i+1} + 1).$$

iv) The number of self-dual $\boldsymbol{F}_4$-codes of length ℓ containing a given nonzero codeword of length ℓ and even Hamming weight is given by

$$M(4, \ell) = \prod_{i=0}^{\frac{\ell}{2}-2} (2^{2i+1} + 1).$$

Proof: i) and iii) are well-known facts, cf. [7]. ii) is an immediate consequence of [6, Theorem 2.1] with $s = 2$. (Note that every self-dual binary code must contain the all-one vector $\mathbf{1}$.) iv) follows from [2, Theorem 1] with $n_1 = \ell$ and $k_1 = 1$. □

Proposition 2.2: Let ℓ be a positive integer divisible by 8.

i) The number of Type II binary codes of length ℓ is given by

$$T(2, \ell) = 2 \prod_{i=1}^{\frac{\ell}{2}-2} (2^i + 1).$$

ii) Let $\boldsymbol{v}$ be a codeword of length ℓ and Hamming weight divisible by 4, other than $\mathbf{0}$ and $\mathbf{1}$. The number of Type II binary codes of length ℓ containing $\boldsymbol{v}$ is given by

$$S(2, \ell) = 2 \prod_{i=1}^{\frac{\ell}{2}-3} (2^i + 1).$$

Proof: i) is found in [7] and ii) is exactly [6, Corollary 2.4]. □

III. Main Result

Let C_1 denote a binary code of length ℓ and C_2 a quaternary code of length ℓ. We construct a binary code C of length 3ℓ by the cubing construction [3]. Define a map

$$\Phi: C_1 \times C_2 \longrightarrow \boldsymbol{F}_2^{3\ell}$$

by the rule

$$\Phi(\boldsymbol{x}, \boldsymbol{a} + \boldsymbol{b}\omega) := (\boldsymbol{x} + \boldsymbol{a}, \boldsymbol{x} + \boldsymbol{b}, \boldsymbol{x} + \boldsymbol{a} + \boldsymbol{b})$$

where $\boldsymbol{a}, \boldsymbol{b}$ are binary vectors of length ℓ, and we write $\boldsymbol{F}_4 = \{0, 1, \omega, \omega^2\}$. Then we can define the code C as $\mathrm{Im}\,(\Phi)$

$$C := \{\Phi(\boldsymbol{x}, \boldsymbol{a} + \boldsymbol{b}\omega) \mid \boldsymbol{x} \in C_1, \boldsymbol{a} + \boldsymbol{b}\omega \in C_2\}.$$

Now a direct calculation shows that

$$\Phi(\boldsymbol{x}, \omega^2(\boldsymbol{a} + \boldsymbol{b}\omega)) = (\boldsymbol{x} + \boldsymbol{a} + \boldsymbol{b}, \boldsymbol{x} + \boldsymbol{a}, \boldsymbol{x} + \boldsymbol{b})$$

is a shift of $\Phi(\boldsymbol{x}, \boldsymbol{a} + \boldsymbol{b}\omega)$ by ℓ places. Therefore, C is ℓ-quasi-cyclic. Furthermore, it is easy to check that C is self-dual if and only if both C_1 and C_2 are, and C is of Type II if and only if C_1 is of Type II and C_2 is self-dual.

We assume henceforth that C is a self-dual code constructed in the above way. Any codeword $\boldsymbol{c}$ in C must necessarily have even Hamming weight. Suppose that $\boldsymbol{c}$ corresponds to the pair $(\boldsymbol{c}_1, \boldsymbol{c}_2)$, where $\boldsymbol{c}_1 \in C_1$ and $\boldsymbol{c}_2 \in C_2$. Since C_1 and C_2 are self-dual, it follows that

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: matlings@nus.edu.sg).

P. Solé is with CNRS, I3S, ESSI, 06903 Sophia Antipolis, France (e-mail: ps@essi.fr).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.809501

$\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ must both have even Hamming weights. When $\boldsymbol{c} \neq \mathbf{0}$, there are three possibilities for the pair $(\boldsymbol{c}_1, \boldsymbol{c}_2)$:

1) $\boldsymbol{c}_1 \neq \mathbf{0}, \boldsymbol{c}_2 \neq \mathbf{0}$;
2) $\boldsymbol{c}_1 = \mathbf{0}, \boldsymbol{c}_2 \neq \mathbf{0}$;
3) $\boldsymbol{c}_1 \neq \mathbf{0}, \boldsymbol{c}_2 = \mathbf{0}$.

We try to enumerate the number of words $\boldsymbol{c}$ in each of these categories for a given weight d (d even).

For type 2, if the Hamming weight of $\boldsymbol{c}$ is d, then $\boldsymbol{c}_2$ has Hamming weight $d/2$. Since $\boldsymbol{c}_2$ has even Hamming weight, it follows that d is divisible by 4 in order for this case to occur. It is easy to see that the number $A_2(\ell, d)$ of such words $\boldsymbol{c}$ is given by $\binom{\ell}{d/2}3^{d/2}$ $(4|d)$. For d not divisible by 4, set $A_2(\ell, d) = 0$.

The argument to obtain the number of words of type 3 is similar. It is easy to show that the number $A_3(\ell, d)$ of such words is given by $\binom{\ell}{d/3}$ $(6|d)$. When d is not divisible by 6, $A_3(\ell, d) = 0$.

For $A_1(\ell, d)$, the number of words of type 1, we simply give an upper bound. The total number of words in $\boldsymbol{F}_2^{3\ell}$ of weight d is $\binom{3\ell}{d}$, so

$$A_1(\ell, d) \leq \binom{3\ell}{d} - A_2(\ell, d) - A_3(\ell, d).$$

Combining the preceding observations and Proposition 2.1, the number of self-dual binary ℓ-quasi-cyclic codes of length 3ℓ whose minimum weight is $< d$ is bounded above by

$$\sum_{e<d,\, e \text{ even}} (A_1(\ell, e)M(2, \ell)M(4, \ell) + A_2(\ell, e)N(2, \ell)M(4, \ell) + A_3(\ell, e)M(2, \ell)N(4, \ell)).$$

Theorem 3.1: Let ℓ be an even integer and let d be the largest even integer such that

$$\sum_{\substack{e<d \\ e\equiv 0 \bmod 2}} \binom{3\ell}{e} + \left(\sum_{\substack{e<d \\ e\equiv 0 \bmod 4}} \binom{\ell}{e/2}3^{e/2}\right)2^{\frac{\ell}{2}-1} + \left(\sum_{\substack{e<d \\ e\equiv 0 \bmod 6}} \binom{\ell}{e/3}\right)2^{\ell-1} \leq (2^{\frac{\ell}{2}-1}+1)(2^{\ell-1}+1).$$

Then there exists a self-dual binary ℓ-quasi-cyclic code of length 3ℓ with minimum weight of at least d.

If we are interested only in Type II ℓ-quasi-cyclic codes, using Proposition 2.2, we see easily that the number of Type II binary ℓ-quasi-cyclic codes of length 3ℓ whose minimum weight is $<d$ is bounded above by

$$\sum_{e<d,\, e\equiv 0 \bmod 4} (A_1(\ell, e)S(2, \ell)M(4, \ell) + A_2(\ell, e)T(2, \ell)M(4, \ell) + A_3(\ell, e)S(2, \ell)N(4, \ell)).$$

Theorem 3.2: Let ℓ be divisible by 8 and let d be the largest multiple of 4 such that

$$\sum_{\substack{e<d \\ e\equiv 0 \bmod 4}} \binom{3\ell}{e} + \left(\sum_{\substack{e<d \\ e\equiv 0 \bmod 4}} \binom{\ell}{e/2}3^{e/2}\right)2^{\frac{\ell}{2}-2} + \left(\sum_{\substack{e<d \\ e\equiv 0 \bmod 12}} \binom{\ell}{e/3}\right)2^{\ell-1} \leq (2^{\frac{\ell}{2}-2}+1)(2^{\ell-1}+1).$$

Then there exists a Type II binary ℓ-quasi-cyclic code of length 3ℓ with minimum weight of at least d.

IV. Asymptotic Analysis

We will require the celebrated entropy function

$$H(x) := -x\log_2(x) - (1-x)\log_2(1-x)$$

defined for $x \in (0, 1)$ and of constant use in estimating binomial coefficients of large arguments [5, pp. 309–310].

We are now in a position to state and prove the asymptotic versions of Theorems 3.1 and 3.2.

Theorem 4.1: There exists an infinite family of self-dual quasi-cyclic binary codes C_i of length $3\ell_i$ and of distance d_i such that the limit δ of $d_i/3\ell_i$ for large i exists and is bounded below as

$$\delta \geq H^{-1}(1/2) = 0.110\cdots.$$

Proof: The right-hand side (RHS) of the inequality of Theorem 3.1 is plainly of the order of $2^{3\ell/2}$ for large ℓ. We compare this in turn to each of the three summands in the left-hand side (at the price of a more stringent inequality, congruence conditions on the summation range are neglected). By [5, Ch. 10, Corollary 9], for large ℓ (with $\mu = \delta$ and $n = \ell$), the first and third summands are of order $2^{3\ell H(\delta)}$ and $2^{\ell+\ell H(\delta)}$, respectively. They both are of the order of the RHS for $H(\delta) = 1/2$. By [5, Ch. 10, Lemma 7], for large ℓ (with $\lambda = \delta$ and $n = \ell$), the second summand is of order $2^{\ell f(3\delta/2)}$ for $f(t) := 0.5 + t\log_2(3) + H(t)$, which is of the order of the RHS for

$$\delta = 0.1762\cdots$$

a value $> H^{-1}(1/2)$. □

Similarly, for doubly even codes, we have the following.

Theorem 4.2: There exists an infinite family of Type II quasi-cyclic binary codes C_i of length $3\ell_i$ and of distance d_i such that the limit δ of $d_i/3\ell_i$ for large i exists and is bounded below as

$$\delta \geq H^{-1}(1/2) = 0.110\cdots.$$

Proof: Since we neglected the congruence conditions in the preceding analysis, the calculations are exactly the same. □

References

[1] T. Kasami, "A Gilbert–Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inform. Theory*, vol. IT-20, p. 679, 1974.

[2] J. H. Conway, V. Pless, and N. J. A. Sloane, "Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16," *IEEE Trans. Inform. Theory*, vol. IT–25, pp. 312–322, 1979.

[3] G. D. Forney, "Coset codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, 1988.

[4] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2751–2760, Nov. 2001.

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

[6] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self-dual codes exist," *Discr. Math.*, vol. 3, pp. 153–162, 1972.

[7] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. I, pp. 177–294.