QUASI-TWISTED CODES AS CONTRACTIONS OF QUASI-CYCLIC CODES

FERRUH ÖZBUDAK AND BUKET ÖZKAYA

1. Quasi-Twisted Codes

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power. Let m be throughout a positive integer with $\gcd(m,q)=1$. For a fixed $\lambda \in \mathbb{F}_q \setminus \{0\}$, let r be the smallest divisor of $q-1$ with $\lambda^r = 1$ and let α be a primitive rm^{th} root of unity such that $\alpha^m = \lambda$. Then, $\xi := \alpha^r$ is a primitive m^{th} root of unity and the roots of $x^m - \lambda$ are of the form $\alpha, \alpha\xi, \ldots, \alpha\xi^{m-1}$. Henceforth, let $\Omega := \{\alpha\xi^k : 0 \le k \le m-1\} = \{\alpha^{1+kr} : 0 \le k \le m-1\}$ be the set of all m^{th} roots of λ and let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_q$ that contains Ω (equivalently, $\mathbb{F} = \mathbb{F}_q(\alpha)$ so that $\mathbb{F}$ is the splitting field of $x^{rm}-1$).

Now let ℓ be a positive integer. A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is called a λ-quasi-twisted (λ-QT) code of index ℓ and co-index m if it is invariant under the λ-constashift of codewords by ℓ positions and ℓ is the least positive integer with this property. In particular, if $\ell = 1$, then C is a λ-constacyclic code, and if $\lambda = 1$ or $q = 2$, then C is a quasi-cyclic (QC) code of index ℓ. If we view a codeword $\mathbf{c} \in C$ as an $m \times \ell$ array

$$\mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix}, \tag{1}$$

then being invariant under λ-constashift by ℓ positions in $\mathbb{F}_q^{m\ell}$ corresponds to being closed under row λ-constashift in $\mathbb{F}_q^{m\times\ell}$.

Assume that $x^m - \lambda$ factors into irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - \lambda = f_1(x) f_2(x) \cdots f_s(x). \tag{2}$$

Since m is relatively prime to q, there are no repeating factors in (2). For each $i \in \{1,2,\ldots,s\}$, let u_i be the smallest nonnegative integer such that $f_i(\alpha\xi^{u_i}) = 0$. The $\mathbb{F}_q$-conjugacy class (or the q-cyclotomic class) containing $\alpha\xi^{u_i}$ in Ω is defined as

$$\left[\alpha\xi^{u_i}\right] = \left\{\alpha\xi^{u_i}, \alpha^q\xi^{qu_i}, \alpha^{q^2}\xi^{q^2u_i}, \ldots, \alpha^{q^{e_i-1}}\xi^{q^{e_i-1}u_i}\right\} \subseteq \Omega, \tag{3}$$

where $e_i = \deg(f_i)$ and therefore $\left[\alpha\xi^{u_i}\right]$ contains all roots of the irreducible polynomial f_i, for each i. Note that Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes.

It is known that an arbitrary codeword $\mathbf{c} \in C$ can be written as an $m \times \ell$ array in the form (see [7])

$$\mathbf{c} = \frac{1}{m} \begin{pmatrix} \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-0} \xi^{-0u_i} \right) \right)_{0 \le t \le \ell-1} \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-1} \xi^{-u_i} \right) \right)_{0 \le t \le \ell-1} \\ \vdots \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q} \left(\kappa_{i,t} \alpha^{-(m-1)} \xi^{-(m-1)u_i} \right) \right)_{0 \le t \le \ell-1} \end{pmatrix} \tag{4}$$

such that $\kappa_i = (\kappa_{i,0}, \ldots, \kappa_{i,\ell-1}) \in C_i$, for all i, where C_i's are linear codes of length ℓ called the *constituents* of the QT code C.

2. Cyclic Codes Contracted to Constacyclic Codes

It was shown in [1] that constacyclic codes are contractions of cyclic codes. Moreover, under certain assumptions, the contracted constacyclic code has the same dimension as the long cyclic code. This yields the explicit construction of good constacyclic codes with a prescribed minimum distance and rate. Several minimum distance bounds known for cyclic codes based on their zero sets can be used for the design of such codes.

Assume the notation above and let $\ell = 1$ so that $C \subseteq \mathbb{F}_q^m$ is a λ-constacyclic code of length m. Consider the principal ideal $I = \langle x^m - \lambda \rangle$ of $\mathbb{F}_q[x]$ and define the residue class ring $R := \mathbb{F}_q[x]/I$. For an element $\mathbf{c} \in \mathbb{F}_q^m$, we associate an element of R as

$$\begin{array}{ccc} \mathbb{F}_q^m & \longrightarrow & R \\ \mathbf{c} = (c_0, c_1, \ldots, c_{m-1}) & \longmapsto & c(x) := c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} \end{array} .$$

Observe that the λ-constashift invariance in $\mathbb{F}_q^m$ corresponds to being closed under multiplication by x in R. Therefore, the above map yields an isomorphism and any λ-constacyclic code $C \subseteq \mathbb{F}_q^m$ can be viewed as an ideal of R. Since every ideal in R is principal, there exists a unique monic polynomial $g(x) \in R$ such that $C = \langle g(x) \rangle$, *i.e.*, each codeword $c(x) \in C$ is of the form $c(x) = a(x)g(x)$, for some $a(x) \in R$. The polynomial $g(x)$, which is a divisor of $x^m - \lambda$, is called the *generator polynomial* of C. Given the λ-constacyclic code $C = \langle g(x) \rangle$, the set of roots of its generator polynomial, say

$$L := \{ \alpha \xi^k \ : \ g(\alpha \xi^k) = 0 \} \subseteq \Omega,$$

is called the *zero set* of C. Note that $\alpha \xi^k \in L$ implies $\alpha^q \xi^{qk} \in L$, for each k, where $\alpha^q \xi^{qk} = \alpha \xi^{k'}$ with $k' = \frac{q-1}{r} + qk \mod m$. Therefore, the zero set L is a union of q-cyclotomic cosets $\left[\alpha \xi^{u_i} \right]$ given as in (3) provided that the minimal polynomial of $\alpha \xi^{u_i}$ divides the generator polynomial $g(x)$. We define the *basic zero set* of C as $\mathrm{BZ}(C) = \left\{ \alpha \xi^{u_i} : \left[\alpha \xi^{u_i} \right] \subseteq L \right\}$. It is not hard to see that if $\alpha \xi^k$ is a zero of C then $\alpha \xi^{-k}$ is a zero of $C^\perp$, which is generated by the reciprocal polynomial of $\frac{x^m - \lambda}{g(x)}$. After this preparation, observe that the case $\ell = 1$ in the trace representation (4) gives us the trace representation of a λ-constacyclic code of length m, in the sense of the following

formulation: If $\mathrm{BZ}(C^\perp) = \left\{\alpha\xi^{-u_i} : \left[\alpha\xi^{-u_i}\right] \subseteq \Omega \setminus L\right\}$, then

$$C = \left\{ \left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q} \left(\sum_{i=1}^{s} \kappa_i \alpha^{-j} \xi^{-ju_i} \right) \right)_{0 \le j \le m-1} \right\},$$

where $\kappa_i \in \mathbb{F}$ if $\alpha\xi^{-u_i} \in \mathrm{BZ}(C^\perp)$ and $\kappa_i = 0$ otherwise. Hence, the columns of any codeword in the λ-QT code viewed as in (4) lie in the q-ary λ-constacyclic code D of length m with $\mathrm{BZ}(D^\perp) = \{\alpha\xi^{-u_1}, \ldots, \alpha\xi^{-u_s}\}$.

We now translate the findings in [1] into our notation provided above.

Theorem 2.1. [1, Theorems 11 and 12] *If C is a λ-constacyclic code of length m and dimension k over $\mathbb{F}_q$ such that $\gcd(m, q) = 1$ and $\lambda^r = 1$, then there exists a q-ary cyclic code D of length rm, dimension k and minimum distance $r \cdot d(C)$ with codewords of the form $(\mathbf{c}, \lambda^{-1} \cdot \mathbf{c}, \ldots, \lambda^{-(r-1)} \cdot \mathbf{c})$, where $\mathbf{c} \in C$. Conversely, let D be a q-ary cyclic code of length rm such that $\gcd(m, q) = 1$ and $r \mid q - 1$ with $\lambda^r = 1$, for some nonzero element $\lambda \in \mathbb{F}_q$, and let $BZ(D^\perp) = \{\alpha^{-v_1}, \ldots, \alpha^{-v_t}\}$ such that $-v_1 \equiv -v_2 \equiv \cdots \equiv -v_t \mod r$. Then, the codewords of D are of the form $(\lambda^{r-1} \cdot \mathbf{c}, \lambda^{r-2} \cdot \mathbf{c}, \ldots, \lambda \cdot \mathbf{c}, \mathbf{c})$, where $\mathbf{c}$ is a codeword of a q-ary λ-constacyclic code C of length m and minimum distance $\frac{d(D)}{r}$. Moreover, C and D have the same dimensions over $\mathbb{F}_q$.*

We are aimed at generalizing this relation and show that quasi-twisted codes are contractions of quasi-cyclic codes. Our main tool is the closely related algebraic structure of quasi-cyclic and quasi-twisted codes, studied in [4, 6, 7]. A few minimum distance bounds for quasi-cyclic codes are known ([3, 5]). More recently, a generalized spectral bound on the minimum distance of a quasi-twisted code was proven in [2]. Based on these results, our purpose is to derive good quasi-twisted codes by contracting quasi-cyclic codes with a designed minimum distance. We also consider some further generalizations.

References

[1] J. Bierbrauer, "The theory of cyclic codes and a generalization to additive codes", *Des. Codes Cryptog.*, vol. 25, 189–206, 2002.

[2] M. F. Ezerman, J. M. Lampos, S. Ling, B. Özkaya and J. Tharnnukhroh, "A comparison of distance bounds for quasi-twisted codes", *IEEE Trans. Inf. Theory*, vol. 67, no. 10, 6476 – 6490, 2021.

[3] C. Güneri and F. Özbudak, "A bound on the minimum distance of quasi-cyclic codes", *SIAM J. Discrete Math*, vol. 26, no. 4, 1781–1796, 2012.

[4] C. Güneri and F. Özbudak, "The concatenated structure of quasi-cyclic codes and an improvement of Jensen's bound", *IEEE Trans. Inform. Theory*, vol. 59, no. 2, pp. 979–985, 2013.

[5] J.M. Jensen, "The concatenated structure of cyclic and abelian codes", *IEEE Trans. Inform. Theory*, vol. 31, no. 6, 788–793, 1985.

[6] Y. Jia, "On quasi-twisted codes over finite fields", *Finite Fields Appl.*, vol. 18, 237–257, 2012.

[7] J. Lv and J. Gao, "A minimum distance bound for 2-dimension λ-quasi-twisted codes over finite fields", *Finite Fields Appl.*, vol. 51, 146–167, 2018.