Some recent progress on cyclic codes

Tao Feng (tfeng@zju.edu.cn)
Department of Mathematics, Zhejiang University

Fq11, Otto-von-Guericke University
Magdeburg, July 23, 2013
1. Two-weight projective cyclic codes: Vega

2. Cyclic codes with two primitive nonzeros: Sarwate
A projective code is a linear code such that the minimum weight of its dual code is at least 3. A cyclic code is irreducible if its check polynomial is irreducible.

When a cyclic code has exactly one nonzero weight, a nice characterization is given by Vega. The class of two-weight cyclic codes was extensively studied. Schmidt and white obtained the necessary and sufficient conditions for an irreducible cyclic code to have at most two weights, and they also explored the connections with other combinatorial objects.
It was once conjectured that two-weight projective cyclic codes must be irreducible. Wolfmann (2005) proved that this is true when $q = 2$, but false when $q > 2$. To be more specific, he proved that if $C$ is a two-weight projective cyclic code of dimension $k$ over $\mathbb{F}_q$, then either

- $C$ is irreducible, or
- $q > 2$, $C$ is the direct sum of two one-weight irreducible cyclic codes of length $n = \lambda \frac{q^k - 1}{q - 1}$, where $\lambda | q - 1$ and $\lambda \neq 1$.

Additionally, the two nonzero weights are $\lambda q^{k-1}$ and $(\lambda - 1)q^{k-1}$.

After Wolfmann’s work, several infinite families of two-weight cyclic codes of the second type were discovered, and a unified explanation is given by Vega.
Vega’s Theorem

Let $a_1, a_2, \nu$ be integers such that $a_1 q^i \not\equiv a_2 \pmod{q^k - 1}$ for all $i \geq 0$, $\nu = \gcd(a_1 - a_2, q - 1)$ and $a_2 \in \mathbb{Z}_\Delta$, where $\tilde{a}_2$ is the inverse of $a_2$ in $\mathbb{Z}_\Delta^*$, $\Delta = \frac{q^{k-1}}{q-1}$. For an integer $\ell$ which divides $\gcd(a_1, a_2, q - 1)$, we set $\lambda = \frac{(q-1)\ell}{\gcd(a_1, a_2, q-1)}$, $n = \lambda \Delta$ and $\mu = \frac{q-1}{\lambda}$. Suppose that at least one of the following two conditions holds:

- $p = 2$, $k = 2$, $\nu = 1$, and $a_1$ is a unit in the ring $\mathbb{Z}_\Delta$, or
- for some integer $j$, $1 + \tilde{a}_2(a_1 - a_2) \equiv p^j \pmod{\nu \Delta}$.

Then $\mu | \nu$, $\lambda > \nu / \mu$, and the following four assertions are true:

- $h_{a_1}(x)$, $h_{a_2}(x)$ are the check polynomials for two different one-weight $[n, k]$ cyclic codes;

- If $C$ is the cyclic codes with check polynomial $h_{a_1}(x)h_{a_2}(x)$, then $C$ is an $[n, 2k]$ two-weight cyclic code with nonzero weights $\lambda q^{k-1}$ and $(\lambda - \nu / \mu) q^{k-1}$;
Moreover, $C$ is a projective code if and only if $v = \mu$. Here $h_a(x)$ is the minimal polynomial of $\gamma^a$ over $\mathbb{F}_q$. □

Vega showed that $\gcd(a, \Delta) = 1$ if and only if $h_a(x)$ is the check polynomial for a one-weight cyclic code.

It is not hard to show that under condition (1) in the above theorem, the code $C$ can not be projective. We are able to prove the following characterization of two-weight projective cyclic codes.
Let $C$ be an $[n, k]$ two-weight projective cyclic code over $\mathbb{F}_q$ with $\gcd(n, q) = 1$. Then $C$ is either irreducible, or the direct sum of two one-weight irreducible cyclic subcodes of the same dimension. Let $\gamma$ be a fixed primitive element of $\mathbb{F}_{q^k}$. In the latter case, $q > 2$, and there exist integers $a_1, a_2$ such that

- $a_1 \not\equiv a_2 q^j \pmod{q^k - 1}$ for any integer $j$;
- $a_1, a_2 \in \mathbb{Z}_\Delta^*$;
- $\gcd(a_1, a_2, q - 1) = \gcd(a_1 - a_2, q - 1) = \frac{r-1}{n}$;
- $1 + \tilde{a}_2(a_1 - a_2) \equiv p^j \pmod{v\Delta}$ for some integer $j$, where $\tilde{a}_2$ is the inverse of $a_2$ in $\mathbb{Z}_\Delta^*$.

Moreover, the product $h_{a_1}(x)h_{a_2}(x)$ is the check polynomial of the cyclic code $C$. 

The projective case: characterization (F., 2012)
Based on computer search evidence, Vega conjectured that all two-weight cyclic codes of the aforementioned type are the known ones. Our result indicates that this is the case if the code is projective. The proof makes use of group rings, characters, Gauss sums, Stickelberger’s theorem, multipliers of difference sets and detailed analysis.
A related conjecture: Schmidt-White

A two-weight code is a code with two nonzero Hamming weights. Typical examples are the subfield codes and semiprimitive codes. Write $f = \operatorname{ord}_v(q)$, $m = fs$, and let $c(m, v)$ denote the $q$-ary irreducible cyclic code of length $v$ with an check polynomial of degree $m$.

**Theorem (Schmidt-White)** The irreducible cyclic code $c(m, v)$ is a two-weight code iff there exists an integer $k$ satisfying the three conditions: (1) $k | v - 1$; (2) $k2^{s\theta} \equiv \pm 1 \pmod{v}$; (3) $k(v - k) = (v - 1)2^{s(f-2\theta)}$.

**Conjecture (Schmidt-White)**: All the irreducible two-weight cyclic codes consists of the two infinite families mentioned above and eleven sporadic examples.
References

2. Cyclic codes with two primitive nonzeros: conjectures

We refer to the webpage of Phillipe Langevin (http://langevin.univ-tln.fr/project/spectrum/) for the the Walsh spectrums of all the power functions $x^d$ in the fields $\mathbb{F}_{2^m}$, for all integers $m < 26$, and all invertible (modulo $2^m - 1$) exponent $d$. You can also find some other interesting conjectures there.
Walsh spectrum

Let $q$ be a power of a prime $p$, and $k$ be an integer such that $\gcd(d, q - 1) = 1$. The Walsh spectrum $\text{Spec}(k)$ consists of the following Weil sums

$$W_{q,k}(a) := \sum_{x \in \mathbb{F}_q} \xi_p^{\frac{2\pi i}{p} \text{Tr}(x^k + ax)}, \quad a \in \mathbb{F}_q^*.$$

We shall ignore $q$ when it causes no confusion.

The Walsh spectrum is related to several concepts: cross-correlation of m-sequences, weights in certain cyclic codes with two primitive zeros, sizes of intersections of certain subsets of $PG(r - 1, 2)$ with the hyperplanes (in the case $q = 2^r$). A nice exposition of these connections are given by D. Katz (2012).
Connections with codes \((p = 2)\)

Let \(q = 2^m\), \(L = F_q\), and \(\alpha\) be a primitive element of \(L\). Let \(C_{1,k}\) be the cyclic code of length \(q - 1\) with two zeros \(\alpha\) and \(\alpha^k\), where \(k\) is an integer such that \(1 \leq k \leq q - 2\), \(\gcd(k, q - 1) = 1\). The codewords of \(C_{1,k}^\perp\) are

\[
c(a, b) = (\Tr(a + b), \Tr(a\alpha^k + b\alpha), \cdots, \Tr(a\alpha^{(q-2)k} + b\alpha^{q-2}))
\]

with \(a, b \in L\).

When exactly one of \(a, b\) is 0, the codeword \(c(a, b)\) has weight \(q/2\). When \(a, b\) are both nonzeros, \(c(a, b)\) has weight

\[
\frac{1}{2} \sum_{i=0}^{q-2} (1 - (-1)^{\Tr(a\alpha^{ki} + b\alpha^i)}) = \frac{q}{2} - \frac{1}{2} W_k(ba^{-1/k}).
\]

Therefore, to study the weights of \(C_{1,k}^\perp\) is actually to compute \(\Spec(k)\).
It is also equivalent to the determination of the crosscorrelation function of two binary m-sequences of length $q - 1$. If two m-sequences of length $q - 1$ differ by a cyclic shift and a decimation by $k$, then their cross-correlation function takes the values in $-1 + \text{Spec}(k)$. 
In 1976, Helleseth proved that the set $\text{Spec}(k)$ has at least three values if and only if $k$ is not a power of 2. At the end of the same paper, he proposed the following two conjectures.

**Conjecture 1.** If $q > 2$ and $k \equiv 1 \pmod{p-1}$, then $W_{q,k}(a) = 0$ for some $a \in \mathbb{F}_q^*$. 

**Conjecture 2.** $\text{Spec}(k)$ can not be three valued when $m$ is a power of 2, $\gcd(k, p^m - 1) = 1$.

When $p = 2$, the second conjecture is now proved in a series of papers by: Calderbank, McGuire, Poonen and Rubinstein (1996), F. (2011), D. Katz (2012). Recently D. Katz proved the $p = 3$ case (see his talk). There is not much progress on the second conjecture to my knowledge.
Another two conjectures ($p = 2$)

**Conjecture 3 (Michko).** If $m$ is odd, then $\# \text{Spec}(k) \neq 4$ if $\gcd(k, 2^m - 1) = 1$.

**Conjecture 4 (Sarwate).** If $m = 2t$, then $\max(\text{Spec}(k)) \geq 2^{t+1}$. 
3. Some progress on Sarwate’s conjecture

**Conjecture (coding version).** Let $m = 2t$, and let $C_d$ be the $[2^m - 1, 2m]$ binary cyclic code with two nonzeros $\alpha^{-1}$ and $\alpha^{-d}$ ($\gcd(d, 2^m - 1) = 1$), where $\alpha$ is a primitive element of $\mathbb{F}_{2^m}$. Then the minimum distance of $C_d$ is $\leq 2^{m-1} - 2^t$.

**Conjecture (spectrum version).** If $m = 2t$, then $\max(\text{Spec}(k)) \geq 2^{t+1}$.

I will talk about some recent progress on the Sarwate conjecture (joint work with Ka Hin Leung, Qing Xiang), which appeared in the special volume of Science Sinica Mathematics on $C^3$. 
The main theorem

Let $m = 2t$, $\mathbb{F} = \mathbb{F}_{2^m}$ and let $C_d$ be the $[2^m - 1, 2m]$ binary cyclic code with two nonzeros $\alpha^{-1}$ and $\alpha^{-d}$ ($gcd(d, 2^m - 1) = 1$), where $\alpha$ is a primitive element of $\mathbb{F}$. Then the minimum distance of $C_d$ is $< 2^{m-1} - 2^{t-1} - 2\lfloor t/2 \rfloor - 1$. That is, there is a nonzero $a \in \mathbb{F}$ such that $W_d(a) > 2^t + 2^\lfloor t/2 \rfloor$. 
Proof:

For any nonzero $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, by direct calculations we have

$$\sum_{a \in \mathbb{F}_{2^t}} W_d(a) \left(1 - (-1)^{\text{Tr}_m(ba)} \epsilon_b \right) = 2^m + 2^t |M_b|, \quad (1)$$

where $M_b = \sum_{x \in \mathbb{F}_{2^t}} (-1)^{\text{Tr}_m((x+b)^d)}$ and $\epsilon_b = \pm 1$ is chosen such that $\epsilon_b M_b = -|M_b|$. For $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, it will be convenient to introduce a function $p_b$ on $\mathbb{F}_{2^t}$ defined by

$$p_b(a) := 1 - (-1)^{\text{Tr}_m(ba)} \epsilon_b, \quad \forall a \in \mathbb{F}_{2^t}.$$  

Then for $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, we have $\sum_{a \in \mathbb{F}_{2^t}} p_b(a) = 2^t$, $p_b(a) \geq 0$, and (1) can be rewritten as

$$\sum_{a \in \mathbb{F}_{2^t}} W_d(a)p_b(a) = 2^m + 2^t |M_b|. \quad (2)$$
Next we compute

\[ \sum_{b \in \mathcal{F}} M_b^2 = 2^t \sum_{b \in \mathcal{F}} \sum_{x \in \mathcal{F}^*} (-1)^{\Tr_m((x+b)^d+b^d)} \]

\[ = 2^t |\mathcal{F}| + 2^t \sum_{b \in \mathcal{F}} \sum_{x \in \mathcal{F}^*} (-1)^{\Tr_m(x^d((1+b)^d+b^d))} \]

\[ = 2^t |\mathcal{F}| + 2^t \left( 2^t \cdot |\{ b \in \mathcal{F} \mid \Tr_{m/t}((1+b)^d + b^d) = 0 \}| - |\mathcal{F}| \right) \]

\[ = 2^{2t} \cdot |\{ b \in \mathcal{F} \mid (1+b)^d + b^d \in \mathcal{F}^2 \}|. \]

Since \( M_b = 2^t \) if \( b \in \mathcal{F}^2 \), we thus have

\[ \sum_{b \in \mathcal{F} \setminus \mathcal{F}^2} M_b^2 = 2^{2t} \cdot |\{ b \in \mathcal{F} \setminus \mathcal{F}^2 \mid (1+b)^d + b^d \in \mathcal{F}^2 \}|. \]
Let \( c \in \mathbb{F}^* \) be an element of order \( 2^t + 1 \). Then a system of coset representatives of \((\mathbb{F}_{2t}, +)\) in \((\mathbb{F}, +)\) is given by \( uc, u \in \mathbb{F}_{2t} \). Since \( M_{b+x} = M_b \) for any \( x \in \mathbb{F}_{2t} \), and \( \mathbb{F} \setminus \mathbb{F}_{2t} = \bigcup_{u \in \mathbb{F}^*_{2t}} (uc + \mathbb{F}_{2t}) \), we get

\[
\sum_{u \in \mathbb{F}^*_{2t}} M_{uc}^2 = 2^t \cdot |\{ b \in \mathbb{F} \setminus \mathbb{F}_{2t} \mid (1 + b)^d + b^d \in \mathbb{F}_{2t} \}|. \quad (3)
\]
If $u \in \mathbb{F}^*_{2^t}$, we have

$$M_{uc} = \sum_{x \in \mathbb{F}_{2^t}} (-1)^{\text{Tr}_m((x+uc)^d)}$$

$$= \sum_{x \in \mathbb{F}_{2^t}} (-1)^{\text{Tr}_t\left(u^d\left((x+c)^d + (x+c^{2^t})^d\right)\right)}$$

$$= \sum_{z \in R_d} \psi_{ud}(z),$$

where $R_d$ denotes the multiset $"(x + c)^d + (x + c^{2^t})^d, x \in \mathbb{F}_{2^t}"$ (each element of $R_d$ indeed belongs to $\mathbb{F}_{2^t}$), and $\psi_{ud}$ is the canonical additive character of $\mathbb{F}_{2^t}$. 
We write the multiset $R_d$ as a group ring element:

$$R_d = \sum_{g \in \mathbb{F}_{2^t}} a_g [g] \in \mathbb{Q}[(\mathbb{F}_{2^t}, +)].$$

Then $\sum_{a \in \mathbb{F}_{2^t}} a_g = 2^t$, each $a_g$ is a nonnegative integer, and for $u \in \mathbb{F}_{2^t}^*$, $M_{uc} = \psi_{ud}(R_d)$.

Furthermore note that each coefficient $a_g$ of $R_d$ must be even. We compute the coefficient of the identity (i.e., the zero element of $\mathbb{F}_{2^t}$) in $R_d R_d^{(-1)}$ in two ways, where $R_d^{(-1)} = \sum_{g \in \mathbb{F}_{2^t}} a_g [-g]$. In fact, we have $R_d^{(-1)} = R_d$ here.
On the one hand, this coefficient is equal to

\[
\sum_{g \in \mathbb{F}_{2^t}} a_g^2 \geq 2^2 \cdot 2^{t-1} = 2^{t+1}.
\]

On the other hand, by the inversion formula, it is equal to\[
\frac{1}{2^t} \sum_{u \in \mathbb{F}_{2^t}} \psi_u \varphi (R_d)^2 = \frac{1}{2^t} \sum_{u \in \mathbb{F}_{2^t}} M_{uc}^2. \text{ It follows that } \sum_{u \in \mathbb{F}_{2^t}} M_{uc}^2 \geq 2^{2t+1}.
\]

Using (3) we now obtain

\[
(2^t)^2 + 2^t \cdot |\{ b \in \mathbb{F} \setminus \mathbb{F}_{2^t} \mid (1 + b)^d + b^d \in \mathbb{F}_{2^t}\}| \geq 2^{2t+1}.
\]
Therefore

$$|\{ b \in \mathbb{F} \setminus \mathbb{F}_{2t} \mid (1 + b)^d + b^d \in \mathbb{F}_{2t} \}| \geq 2^t,$$

with equality if and only if $R_d$ has size $2^{t-1}$ as a set.

As a consequence, there exists an element $u \in \mathbb{F}_{2t}^*$ such that

$$|M_{uc}| \geq \sqrt{2^{2t}/(2^t - 1)} > 2^{\lfloor t/2 \rfloor}.$$

Using the above element $uc$ as $b$ in Eqn. (2), we see that there is some $a \in \mathbb{F}_{2t}$ such that $W_d(a) > 2^t + 2^{\lfloor t/2 \rfloor}$ by an averaging argument. The proof of the theorem is now complete.
Remark

1. In the case where \( d = 1 + 2^i \), for \( x \in \mathbb{F}_{2^t} \), we have \( \text{Tr}_m((x + b)^d) = \text{Tr}_t(x \nu) + \text{Tr}_m(b^d) \), where \( \nu = \text{Tr}_{m/t}(b)^{2^i} + \text{Tr}_{m/t}(b)^{2^{-i}} \). Choosing \( b \in \mathbb{F} \setminus \mathbb{F}_{2^t} \) such that \( \text{Tr}_{m/t}(b) = 1 \), we have \( \nu = 0 \), and \( |M_b| = 2^t \). We see that this Conjecture is true in this case by using (2).

2. If \( d \) is a Niho exponent, then it is known that \( 2^t | W_d(a) \) for all \( a \in \mathbb{F} \). Combining this divisibility result with our Theorem, we immediately get \( W_d(a) \geq 2^{t+1} \).

3. Assume that \( d = 1 + 2^i + 2^{i+t} \) for some \( i, 0 < i < t - 1 \), and \( \gcd(d, 2^m - 1) = 1 \). Such a \( d \) is not a Niho exponent. We showed that for any \( d \) of the aforementioned form, the Conjecture is true, and specializing to the \( i = 1 \) case, i.e., \( d = 3 + 2^{t+1} \), we determine the Walsh spectrum of \( \text{Tr}(x^d) \) completely.
Thank You!