Patrick Solé joint works with Adel Alahmadi, Cem Gueneri, MinJia Shi, Hatoon Shoaib, Liqin Qian, Rongsheng Wu, Hongwei Zhu

CNRS/LAGA

London, UK, January 2019
M. Shi, L. Qian, P. Solé, On self-dual negacirculant codes of index 2 and 4, Designs Codes & Cryptography, 2017 :1–10
M. Shi, R. Wu, P. Solé, Additive cyclic codes are asymptotically good, IEEE Communications Letters 22(10):
"Are long cyclic codes good"?
Assmus-Mattson-Turyn (1966)

If $C(n)$ is a family of codes of parameters $[n, k_n, d_n]$, the rate $r$ is

$$r = \limsup_{n \to \infty} \frac{k_n}{n},$$

relative distance $\delta$ is

$$\delta = \liminf_{n \to \infty} \frac{d_n}{n}.$$

A family of codes is said to be good iff $r\delta > 0$. 
Negative results

- S. Lin, E. Peterson, Long BCH codes are bad, Information and Control 11(4) :445–451, October 1967
- the most famous class of cyclic codes is bad

⇒ Affine invariant cyclic codes are also bad.

⇒ there are good nonlinear shift-invariant codes


⇒ long dihedral linear codes are good. Proof is involved.


⇒ long quasi-cyclic codes are easier to study than long cyclic codes.

Reason: random coding work better when there are more codes!
Plan

- self-dual **double circulant** codes are dihedral
- they are good by expurgated random coding argument \(\Rightarrow\) new proof of Bazzi-Mitter result
- cyclic codes over extension fields give quasi-cyclic codes by projection on a basis of the extension
- good quasi-cyclic codes give good **additive cyclic** codes over extension fields
- generalizations and extensions: four-circulant codes, **quasi-abelian** codes
Dihedral codes

The **dihedral** group $D_n$, is the group of order $2n$ with two generators $r$ and $s$ of respective orders $n$ and 2 with the relation $srs = r^{-1}$.

$D_n$ is the group of orthogonal transforms (rotation or axial symmetries) of the $n$-gon.

A code of length $2n$ is called **dihedral** if it is invariant under $D_n$ acting transitively on its coordinate places.
Codes over $GF(q)$ of length $2n$ with $n$ odd and coprime to $q$. A code is **double circulant** if its generator matrix $G$ is of the form

$$G = (I, A)$$

$I$ is the identity matrix of order $n$

$A$ is a **circulant** matrix of the same order.

circulant $\Leftrightarrow$ each row obtained from the first by successive shifts.

pure double circulant is different from **bordered** double circulant (add a top row and middle column to $G$)
Self-dual double circulant are dihedral

If $q$ is even, $C$ self-dual double circulant length $2n$ then $C$ is invariant under $D_n$.
The main idea : $A$ is circulant $\Rightarrow \exists$ permutation matrix $P$ such that $PAP = A^t$.
Already observed in
C. Martinez-Perez, W. Willems,
Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good,
Let $T$ denote the shift operator on $n$ positions.  
A linear code $C$ is $\ell$-quasi-cyclic (QC) code if $C$ is invariant under $T^\ell$, i.e. $T^\ell(C) = C$.  
The smallest $\ell$ with that property is called the index of $C$.  
For simplicity we assume that $n = \ell m$ for some integer $m$, sometimes called the co-index.  
The special case $\ell = 1$ gives the more familiar class of cyclic codes.  
Double circulant codes of length $2n$ are, up to equivalence, 2-quasicyclic of co-index $n$.  

Quasi-cyclic codes I
The ring theoretic approach to QC codes is via

\[ R(m, q) = \mathbb{F}_q[x]/\langle x^m - 1 \rangle. \]

Thus cyclic codes of length \( m \) over \( \mathbb{F}_q \) are ideals of \( R(m, q) \) via the polynomial representation.

Similarly QC codes of index \( \ell \) and co-index \( m \) linear codes \( R(m, q) \)
submodules of \( R(m, q)^\ell \).

In the language of polynomials, a codeword of an \( \ell \)-quasi-cyclic code can be written as \( c(x) = (c_0(x), \cdots, c_{\ell-1}(x)) \in R(m, q)^\ell \).

Benefit: use CRT to decompose \( R(m, q) \) into direct sums of local rings
Look at shorter codes over larger alphabets.
Suppose we now there are $\Omega_n$ codes of length $n$ in the family we want to show of relative distance at least $\delta$.

Suppose that there are at most $\lambda_n$ codes in the family containing a given nonzero vector.

Denote by $B(r)$ the volume of the Hamming ball of radius $r$.

If, for $n$ large enough, we can show that

$$B(\lfloor \delta n \rfloor) \lambda_n < \Omega_n$$

then the family will have relative distance $\geq \delta$. 
Algebraic counting

Let $n$ denote a positive odd integer. Assume that $-1$ is a square in $GF(q)$. If $x^n - 1$ factors as a product of two irreducible polynomials over $GF(q)$,

$$x^n - 1 = (x - 1)(x^{n-1} + \cdots + 1),$$

definite number of self-dual double circulant codes of length $2n$ is

\begin{align*}
\Omega_n &= 2\left(q^{\frac{n-1}{2}} + 1\right) & \text{if } q \text{ is odd} \\
\Omega_n &= \left(q^{\frac{n-1}{2}} + 1\right) & \text{if } q \text{ is even}.
\end{align*}

The proof reduces to enumerating hermitian self-dual codes of length $2$ in $GF(q^{\frac{n-1}{2}})$. 
How to have only two factors?

In number theory, Artin’s conjecture on primitive roots states that a given integer \( q \) which is neither a perfect square nor \(-1\) is a primitive root modulo infinitely many primes \( \ell \). It was proved conditionally under the Generalized Riemann Hypothesis (GRH) by Hooley in 1967. In this case, by the correspondence between cyclotomic cosets and irreducible factors of \( x^\ell - 1 \), the factorization of \( x^\ell - 1 \) into irreducible polynomials over \( GF(q) \) contains exactly two factors, one of which is \( x - 1 \).
Covering lemma

Let \( a(x) \) denote a polynomial of \( GF(q)[x] \) coprime with \( x^n - 1 \), and let \( C_a \) be the double circulant code with generator matrix \((1, a)\).

Assume the factorization of \( x^n - 1 \) into irreducible polynomials is \( x^n - 1 = (x - 1)h(x) \).

The following fact was proved first for \( q = 2 \) in Chen, Peterson, Weldon (1969).

With the above assumptions, let \( u \in GF(q)^{2n} \). If \( u \neq 0 \) has Hamming weight \(< n\), then there are at most \( \lambda_n = q \) polynomials \( a \) such that \( u \in C_a \).

The proof uses the CRT decomposition of \( R(n, q) \).
the $q$-ary entropy function is for $0 < t < \frac{q-1}{q}$ by

$$H_q(t) = t \log_q(q - 1) - t \log_q(t) - (1 - t) \log_q(1 - t).$$

If $q$ is not a square, then, under Artin’s conjecture, there are infinite families of self-dual double circulant codes of relative distance

$$\delta \geq H_q^{-1}(\frac{1}{4}).$$

Corollary: long dihedral codes are good.
A linear code of length $N$ is **quasi-twisted** of index $l$ for $l \mid N$, and co-index $m = \frac{N}{l}$ if it is invariant under the power $T^l_\alpha$ of the **constashift** $T_\alpha$ defined as

$$T_\alpha : (x_0, \ldots, x_{N-1}) \mapsto (\alpha x_{N-1}, x_0, \ldots, x_{N-2}).$$

A matrix $A$ over a finite field $\mathbb{F}_q$ is said to be **negacirculant** if its rows are obtained by successive negashifts ($\alpha = -1$) from the first row.

We consider **double negacirculant** (DN) codes over finite fields, that is $[2n, n]$ codes with generator matrices of the shape $(I, A)$ with $I$ the identity matrix of size $n$ and $A$ a negacirculant matrix of order $n$. 

**Double Negacirculant codes I**
The factorization of $x^n + 1$ is in two factors when $n$ is a power of 2. The proof is elementary and relies on *Dickson polynomial* (of the first kind). This is the main difference with the double circulant case.

$$D_n(x, \alpha) = \sum_{p=0}^{\lfloor n/2 \rfloor} \frac{n}{n-p} \binom{n-p}{p} (-\alpha)^p x^{n-2p}.$$ 

The $D_n$ satisfy the Chebyshev’s like identity

$$D_n(u + \alpha/u, \alpha) = u^n + (\alpha/u)^n.$$
If $q$ is an odd integer, and $n$ is a power of 2, then there are infinite families of:

(i) double negacirculant codes of relative distance $\delta$ satisfying $H_q(\delta) \geq \frac{1}{4}$.

(ii) self dual double negacirculant codes of relative distance $\delta$ satisfying $H_q(\delta) \geq \frac{1}{4}$. 

- Double Negacirculant codes III
If you have liked the CRT approach please buy our book!!!!

M. Shi, A. Alahmadi, P. Solé,


More results on

- local rings, Galois rings, chain rings, Frobenius rings, ...
- Lee metric, homogeneous metric, rank metric, RT-metric, ...
- Quasi-twisted codes, consta-cyclic codes, skew-cyclic codes...
A link between QC and cyclic codes

Given a basis $B = \{e_0, e_1, \cdots, e_{\ell-1}\}$ of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$ we can define the following map

$$\phi_B : R(m, q)^\ell \rightarrow R(m, q^\ell)$$

$$(c_0(x), c_1(x), \cdots, c_{\ell-1}(x)) \mapsto \sum_{i=0}^{\ell-1} c_i(x)e_i.$$

This map can be used to construct additive cyclic codes over $\mathbb{F}_{q^\ell}$ from $\ell$-QC codes over $\mathbb{F}_q$.

The reverse map can be used to construct $\ell$-QC codes from cyclic codes over $\mathbb{F}_{q^\ell}$.

The map $\phi_B^{-1}$ has been used since the 1980’s to construct self-dual codes by TOB’s.
Let \( \tilde{C} \) be a quasi-cyclic code of length \( \ell m \) and index \( \ell \) over \( \mathbb{F}_q \). Let \( C = \phi_B^{-1}(\tilde{C}) \) be a cyclic code over \( \mathbb{F}_{q^\ell} \) with respect to a basis \( B = \{e_0, e_1, \cdots, e_{\ell-1}\} \) of \( \mathbb{F}_{q^\ell} \) over \( \mathbb{F}_q \).

Then \( d_{\mathbb{F}_q}(\tilde{C}) \geq d_{\mathbb{F}_{q^\ell}}(C) \).

Equality holds if \( C \) has a minimum weight vector the nonzero components of which are elements of \( B \).
If $C$ is a cyclic code over $\mathbb{F}_{q^\ell}$ then we have

$$\phi_{B^*}^{-1}(C^\perp) = \phi_{B}^{-1}(C)^\perp.$$  

If $B = B^*$, and $C$ is self-dual, then $\phi_{B}^{-1}(C)$ is self-dual. Note that self-dual cyclic codes only exist for even $q^\ell$. If $B = B^*$, and $C$ is LCD, then $\phi_{B}^{-1}(C)$ is LCD.
An **additive cyclic code** over $\mathbb{F}_{q^\ell}$, is an $\mathbb{F}_q$-linear code over the alphabet $\mathbb{F}_{q^\ell}$ that is invariant under the shift $T$. Cyclic codes over $\mathbb{F}_{q^\ell}$, are additive cyclic, but not conversely. See e.g. the dodecacode over $\mathbb{F}_4$. Are useful in quantum error correction. Have deep structure theory.

If $C$ is an $\ell$-quasi-cyclic code of length $n = \ell m$ over $\mathbb{F}_q$ then $\phi_B(C)$ is an additive cyclic code of length $m$ over $\mathbb{F}_{q^\ell}$. The codes in the image of $\phi_B$ need not be $\mathbb{F}_{q^\ell}$-linear in general.
Let \( m = \frac{n}{\ell} \). Assume \( \phi_B(C) \) has constituents \( C_i \) in the CRT decomposition of the ring \( \mathbb{F}_q[x]/(x^m - 1) \).
Write \( \mathbb{F}_{q^\ell} = \mathbb{F}_q(\alpha) \). Denote by \( M_\alpha \) the companion matrix of the minimal polynomial of \( \alpha \).

**Necessary condition:** If \( \phi_B(C) \) is \( \mathbb{F}_{q^\ell} \)-linear then each \( C_i \) is left wholly invariant by \( M_\alpha \).

The theory of invariant subspaces allows us to write each \( C_i \) as a sum of invariant subspaces.

(joint work with Gueneri-Ozdemir to appear in Discrete Math).
Let $q$ be a prime power, and $m$ be a prime.
If $x^m - 1 = (x - 1)u(x)$, with $u(x)$ irreducible over $\mathbb{F}_q[x]$, then for any fixed integer $\ell \geq 2$, there are infinite families of QC codes of length $n\ell$, index $\ell$, rate $1/\ell$ and of relative distance $\delta$,

$$H_q(\delta) \geq \frac{\ell - 1}{\ell}$$

The proof uses expurgated random coding on codes with generator matrices of the form

$$(I, A_1, \cdots, A_{\ell-1}).$$
From QC codes to additive cyclic codes II

For an $\ell$-quasi-cyclic code of length $n = \ell m$ over $\mathbb{F}_q$ of distance $d(C)$, we have the bound on the distance of $d(\phi_B(C))$ given by

$$d(\phi_B(C)) \geq \frac{d(C)}{\ell}.$$ 

The proof is elementary.

Let $c = (c_0, c_1, \ldots, c_{\ell-1}) \in C$, with $c \neq 0$, and with $c_i \in \mathbb{F}_q^m$ for all $i$'s. Put $z = \phi_B(c)$. Then $z = \sum_{i=0}^{\ell-1} c_i e_i$. Consider $z_j$ an arbitrary component of $z$. Thus, by linearity, $z_j = \sum_{i=0}^{\ell-1} c_{ij} e_i$, with $c_{ij}$ component of index $j$ of $c_i$. Since $B$ is a basis $z_j = 0$ entails $c_{ij} = 0$ for all $i$'s. This, in turn, proves that $\ell w(z_j) \geq \sum_{i=0}^{\ell-1} w(c_{ij})$. But

$$w(c) = \sum_{i=0}^{\ell-1} \sum_{j=0}^{m-1} w(c_{ij}),$$

and $w(z) = \sum_{j=0}^{m-1} w(z_j)$. The result follows by summing $m$ inequalities.
Combining good QC codes with the previous bound we obtain
There are infinite families of additive cyclic codes of length
$m \to \infty$ over $\mathbb{F}_{q^\ell}$ of rate $1/\ell$ and relative distance

$$\delta \geq \frac{1}{\ell} H^{-1}_q(1 - 1/\ell).$$
Variations

- from one-generator to two-generator codes
- four circulant codes = two-generator and index 4

$$G = \begin{pmatrix} I_n & 0 & A & B \\ 0 & I_n & -B^T & A^T \end{pmatrix}$$

- From constacyclic codes to quasi-twisted codes (joint work Shi, Guan, Sok)
- From quasi-abelian codes to abelian codes (joint work with Borello, Gueneri, Sacikara)
Let $\lambda \in \mathbb{F}_q^*$ and let $l$ be a positive integer. We define an action of the constashift $T_{\lambda,l}$ on the vectors as

$$T_{\lambda,l}(c_0,0,c_1,0,\cdots,c_0,n-1,c_1,1,\cdots,c_1,n-1,\cdots,c_l-1,0,c_l-1,1,\cdots) = (\lambda c_0,n-1,c_0,0,\cdots,c_0,n-2,\lambda c_1,n-1,c_1,0,\cdots,c_1,n-2,\cdots,c_l-1,n-1,c_l-1,0,\cdots).$$

If $\lambda = 1$, we have the usual cyclic shift. A $(\lambda, l)$-QT code is invariant as a set under the action of $T_{\lambda,l}$. 
Quasi-twisted codes

If for each codeword \( c \in C \), we have \( T_{\lambda,l}(c) \in C \), then the code \( C \) is called a \((\lambda, l)\)-quasi-twisted (QT) code of index \( l \).

By the polynomial correspondence, a \((\lambda, l)\)-QT code of length \( nl \) over \( \mathbb{F}_q \) is identified with a \( \frac{\mathbb{F}_q[x]}{(x^n-\lambda)} \)-submodule of \( \left( \frac{\mathbb{F}_q[x]}{(x^n-\lambda)} \right)^l \).
A matrix $A$ over $\mathbb{F}_q$ is said to be \textit{$\lambda$-circulant} if its rows are obtained by successive $\lambda$-shifts from the first row as follows:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\
\lambda a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\
\lambda a_{n-2} & \lambda a_{n-1} & a_0 & \cdots & a_{n-3} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\lambda a_1 & \lambda a_2 & \lambda a_3 & \cdots & a_0 \end{pmatrix}.$$

A linear code $C$ is called a \textit{four $\lambda$-circulant code} over $\mathbb{F}_q$ if the code $C$ generated by

$$G = \begin{pmatrix} I_n & 0 & A & B \\
0 & I_n & -B^t & A^t \end{pmatrix},$$

where $A, B$ are $\lambda$-circulant matrices and the exponent "$t$" denotes transposition.
Special factorizations of $x^n \pm 1$

**Eq. (1)** $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1)$, where $x - 1$ and $x^{n-1} + \cdots + x + 1$ are irreducible polynomials over $\mathbb{F}_q$.

**Eq. (2)** $x^n + 1 = (x^2 + 1)g_1(x)g_2(x)$, where $x^2 + 1$, $g_1(x)$ and $g_2(x)$ are irreducible polynomials over $\mathbb{F}_q$ and $	ext{deg}(g_1(x)) = \text{deg}(g_2(x))$.

**Eq. (3)** $x^n + 1 = h(x)h^*(x)$, where $h(x)$ and $h^*(x)$ are irreducible polynomials over $\mathbb{F}_q$ and $*$ means reciprocation.

**Eq. (4)** $x^n + 1 = h_1(x)h_1^*(x)h_2(x)h_2^*(x)$, where $h_1(x)$, $h_2(x)$, $h_1^*(x)$ and $h_2^*(x)$ are irreducible polynomials over $\mathbb{F}_q$. 
Asymptotics for quasi-twisted codes

Eq. (1) There exists a family of LCD double circulant codes over $\mathbb{F}_q$ of length $2n$, of relative distance $\delta$, and rate $1/2$, with $H_q(\delta) \geq \frac{1}{2}$.

Eq. (2) There exists a family of LCD double negacirculant codes over $\mathbb{F}_q$ of length $2n$, of relative distance $\delta$, and rate $1/2$, with $H_q(\delta) \geq \frac{1}{4}$; there exists a family of LCD four negacirculant codes over $\mathbb{F}_q$ of length $4n$, of relative distance $\delta$, and rate $1/2$, with $H_q(\delta) \geq \frac{1}{8}$.

Eq. (3) There exists a family of LCD double negacirculant codes over $\mathbb{F}_q$ of length $2n$, of relative distance $\delta$, and rate $1/2$, with $H_q(\delta) \geq \frac{1}{4}$.

Eq. (4) There exists a family of LCD double negacirculant codes over $\mathbb{F}_q$ of length $2n$, of relative distance $\delta$, and rate $1/2$, with $H_q(\delta) \geq \frac{1}{8}$. 
Quasi-abelian codes I

Let $G$ be a finite abelian group of order $n$.
Consider the group algebra $\mathbb{F}_q[G]$, whose elements are formal polynomials $\sum_{g \in G} \alpha_g Y^g$ in $Y$ with coefficients $\alpha_g \in \mathbb{F}_q$.
Note that $\mathbb{F}_q[G]$ can be considered as a vector space over $\mathbb{F}_q$ of dimension $n$.
A code $C$ in $\mathbb{F}_q[G]$ is called an $H$ quasi-abelian code ($H$-QA) of index $\ell$ if $C$ is an $\mathbb{F}_q[H]$-module, where $H$ is a subgroup of $G$ with $[G : H] = \ell$. Let $\{g_1, \ldots, g_\ell\}$ be a fixed set of representatives of the cosets of $H$ in $G$. Note that a QA code of index $\ell$ in $\mathbb{F}_q[G]$ can be seen as an $\mathbb{F}_q[H]$-submodule of $\mathbb{F}_q[H]^\ell$ by the following $\mathbb{F}_q[H]$-module isomorphism.

$$\Phi : \mathbb{F}_q[G] \longrightarrow \mathbb{F}_q[H]^\ell$$

$$\sum_{i=1}^\ell \sum_{h \in H} \alpha_{h+g_i} Y^{h+g_i} \longmapsto \left( \sum_{h \in H} \alpha_{h+g_1} Y^h, \ldots, \sum_{h \in H} \alpha_{h+g_\ell} Y^h \right).$$
Jitman and Ling (2015) call a QA code $C$ strictly QA (SQA) if $H$ is not a cyclic group. Similarly, if $\ell = 1$ and $H$ is not cyclic, we refer to strictly abelian (SA) codes. In this section, we consider the link between QA codes and additive abelian codes. Additive abelian codes have been studied by Cao et al. and Martinez-Moro et al. as a special class of semisimple abelian codes. Semisimple abelian codes are defined as

$$\mathbb{F}_q[x_1, \ldots, x_n]/\langle t_1(x_1), \ldots, t_n(x_n) \rangle$$

submodules in

$$\mathbb{F}_{q^\ell}[x_1, \ldots, x_n]/\langle t_1(x_1), \ldots, t_n(x_n) \rangle.$$ 

Here, $t_i(x_i)$’s are separable polynomials with $\mathbb{F}_q$-coefficients and $\mathbb{F}_{q^\ell}$ denotes an extension field of degree $\ell$ over $\mathbb{F}_q$. Additive abelian codes is the special case of $t_i(x_i) = x_i^{m_i} - 1$. 
Choose a basis $\beta = \{e_1, e_2, \ldots, e_\ell\}$ for $\mathbb{F}_q^\ell$ over $\mathbb{F}_q$. We have the following $\mathbb{F}_q[H]$-module isomorphism

$$
\Phi_\beta : \mathbb{F}_q[H]^\ell \rightarrow \mathbb{F}_q^\ell[H]
$$

$$
\left( \sum_{h \in H} \alpha_{1h} Y^h, \ldots, \sum_{h \in H} \alpha_{\ell h} Y^h \right) \mapsto \sum_{i=1}^\ell (\sum_{h \in H} \alpha_{ih} Y^h) e_i
$$

So, for an $H$-QA code $\mathcal{C}$ of index $\ell$, $\Phi_\beta(\mathcal{C})$ is an $\mathbb{F}_q[H]$-submodule in $\mathbb{F}_q^\ell[H]$, that is an additive abelian code. If $H$ is not cyclic, we call these codes **strictly additive abelian**.
Jitman and Ling showed that the classes of binary self-dual doubly even $H$-QA codes of index $\ell = 2$ and binary $H$-QA LCD codes of index 3 are asymptotically good. In their proof, they consider an infinite family of $H$-QA codes by fixing the index $\ell$. In other words, if $C_{(a,b)}^{(n)}$ is a binary self-dual doubly even asymptotically good family described before, and $C_{(a,b,1)}^{(n)}$ is a binary $H$-QA LCD asymptotically good family described by Jitman-Ling, then the corresponding infinite families of additive strictly abelian codes $\Phi_{\beta}(C_{(a,b)}^{(n)})$ over $\mathbb{F}_4$ and $\mathbb{F}_8$ are asymptotically good.


Conclusion and open problems

- QC and QT codes of low index are good, by random coding
- SD and LCD subclasses are dealt with. Arbitrary hull of given relative dimension?
- additive cyclic codes, additive constacyclic codes, additive abelian codes are good, by mapping from previous
- Are cyclic codes good? : still open after after 50 years!
- Are there QC codes better than VG? still open!
- There are transitive (Stichtenoth 06) and quasi-transitive (Bassa, 2006) codes better than VG. Are they abelian (resp. quasi-abelian)?
Thanks for your attention!