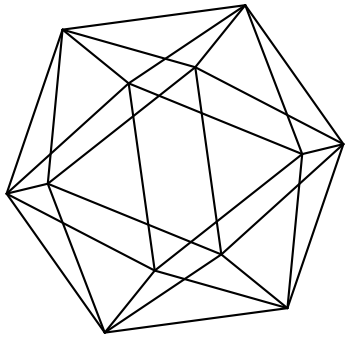
Max-Planck-Institut für Mathematik
Bonn

Asymptotic performance of metacyclic codes

by

Martino Borello
Pieter Moree
Patrick Solé



Max-Planck-Institut für Mathematik
Preprint Series 2019 (37)

Asymptotic performance of metacyclic codes

Martino Borello
Pieter Moree
Patrick Solé

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

LAGA, UMR 7539, CNRS
Université Paris 13 - Sorbonne Paris Cité
Université Paris 8
93526 Saint-Denis
France

Aix Marseille University
CNRS Centrale Marseille, 12 M
13453 Marseille
France

MPIM 19-37

ASYMPTOTIC PERFORMANCE OF METACYCLIC CODES

MARTINO BORELLO, PIETER MOREE, AND PATRICK SOLÉ

Abstract. A finite group with a cyclic normal subgroup N such that G/N is cyclic is said to be metacyclic. A code over a finite field $\mathbb{F}$ is a metacyclic code if it is a left ideal in the group algebra $\mathbb{F}G$ for G a metacyclic group. Metacyclic codes are generalizations of dihedral codes, and can be constructed as quasi-cyclic codes with an extra automorphism. In this paper, we prove that metacyclic codes form an asymptotically good family of codes. Our proof relies on a version of Artin's conjecture for primitive roots in arithmetic progression being true under the Generalized Riemann Hypothesis (GRH).

Keywords. Group code, quasi-cyclic code, metacyclic group, asymptotically good code
MSC(2010). 94A17, 94B05, 20C05

1. Introduction

Metacyclic codes were studied intensively by Sabin in the 1990's [16, 17]. They are (left) ideals in the group ring $\mathbb{F}G(m, s, r)$, where $\mathbb{F}$ is a finite field and $G(m, s, r)$ is the finite group of order ms defined as

$$G(m, s, r) = \langle x, y \mid x^m = 1,\, y^s = 1,\, yx = x^r y \rangle,$$

with $r^s \equiv 1 \pmod{m}$. More recently, their concatenated structure was explored in [5].

In the present paper, we show that for some values of the parameters m, s, r (in particular $s > 1$ fixed, m a prime and $r \neq 1 \pmod{m}$ depending on m), these codes are asymptotically good. This extends results of Bazzi-Mitter, who dealt with $\mathbb{F} = \mathbb{F}_2$ and $G(m, 2, m-1)$, a dihedral group [2], and, partially, Borello-Willems, who considered the case $\mathbb{F} = \mathbb{F}_s$, with both m and s prime. As observed in [3, §4], applying field extensions as in [7, Proposition 12], the result of Bazzi-Mitter can be extended to any field of characteristic 2 and that of Borello-Willems to any field of characteristic m. In our case, the characteristic of the field is not necessarily related to the cardinality of the group, so that we have more freedom in our choice of the alphabet. Moreover, the proof is conceptually simpler. On the other hand, our results rely on a variant of Artin's primitive conjecture (Conjecture 2.1) being true, where the primes are supposed to lie in a progression of the form $1 \pmod{s}$. This is currently only guaranteed on assuming the GRH.

The main idea is to realize metacyclic codes as quasi-cyclic codes with some extra automorphism. Such codes can be enumerated by the Chinese Remainder Theorem (CRT) approach of [12]. This technique regards a quasi-cyclic code of index ℓ as a code of length ℓ over an auxiliary ring. Decomposing the said ring into a direct sum of extension fields by the CRT for polynomials yields a decomposition into codes of length ℓ over these fields. These codes are called constituent codes. The favorable case where there are only two constituents requires, to be realized infinitely many times, to invoke Artin's conjecture. An expurgated random coding argument, similar to the one that proves that double circulant codes are asymptotically good [1], can then be applied.

M. Borello is with LAGA, UMR 7539, CNRS, Université Paris 13 - Sorbonne Paris Cité, Université Paris 8, F-93526, Saint-Denis, France.

P. Moree is with Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

P. Solé is with Aix Marseille University, CNRS, Centrale Marseille, I2M, Marseille, France.

The material is arranged as follows. The next section collects the basic notions and notations needed in the rest of the paper. Section 3 derives the main result. Section 4 concludes the article.

2. Definitions and Notation

2.1. **Quasi-cyclic Codes.** A linear code $\mathcal{C}$ over the finite field $\mathbb{F}$ is said to be **quasi-cyclic** of index ℓ, or ℓ-QC for short, if it is left wholly invariant under the ℓ'th power of the shift. Assume, for convenience, that the length n of $\mathcal{C}$ is $n = \ell m$, for some integer m called the co-index. As is well-known [12], such a code is an R_m-submodule of R_m^ℓ, where R_m denotes the ring $R_m = \mathbb{F}[x]/(x^m - 1)$. A related class of codes is that of **ℓ-circulant** codes, consisting of linear codes of length $n = \ell m$ and dimension m, whose generator matrix is made of circulant blocks of size m. Such codes are coordinate permutation equivalent to ℓ-QC codes. Recall that there is ring isomorphism between circulant matrices of order m and R_m given by $A \mapsto A_{11} + A_{12}x + \cdots A_{1m}x^{m-1}$. Thus, for example, the binary matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

is encoded by that isomorphism as $(1, x + x^2)$.

2.2. **Metacyclic groups.** Let $G(m, s, r)$ denote the group of order ms defined by generators and relations as

$$G(m, s, r) = \langle x, y \mid x^m = 1,\, y^s = 1,\, yx = x^r y \rangle,$$

where r satisfies $r^s \equiv 1 \pmod{*}m$. Such a group is called **metacyclic**, since it has a cyclic normal subgroup $N = \langle x \rangle$ such that the quotient group G/N is also cyclic. When $r = m - 1$ and $s = 2$, we obtain the **dihedral** group D_m of order $2m$,

$$D_m = \langle x, y \mid x^m = 1,\, y^2 = 1,\, yx = x^{-1} y \rangle,$$

while the case $r = 1$ reduces to the abelian group

$$C_m \times C_s = \langle x, y \mid x^m = 1,\, y^s = 1,\, yx = xy \rangle.$$

Here C_i denotes the cyclic group of order i.

2.3. **Group codes.** Let G be a finite group of order n. A **G-code** (or a **group code**) $\mathcal{C}$ over a finite field $\mathbb{F}$ is a left ideal in the group algebra $\mathbb{F}G = \{\sum_{g \in G} a_g g \mid a_g \in \mathbb{F}\}$. Once we choose an ordering of G, we have a $\mathbb{F}$-linear isomorphism $\varphi : \sum_{g \in G} a_g g \mapsto (a_g)_{g \in G}$ between $\mathbb{F}G$ and $\mathbb{F}^n$, and the image of $\mathcal{C}$ is a linear code in $\mathbb{F}^n$. Changing the ordering gives coordinate permutation equivalent codes. The group of permutation automorphism of $\varphi(\mathcal{C})$ contains a transitive subgroup isomorphic to G. It is common practice to identify $\mathcal{C}$ and $\varphi(\mathcal{C})$. A **metacyclic code** is a G-code for $G = G(m, s, r)$ or equivalently a linear code of length ms whose permutation automorphism group contains a transitive subgroup isomorphic to $G(m, s, r)$.

2.4. **The Artin primitive root conjecture for primes in arithmetic progression.** Emil Artin conjectured in 1927 that given a non-zero integer a that is not a perfect square nor -1, there are infinitely many primes m such that a is primitive modulo m. Recall that the Generalized Riemann Hypothesis (GRH) states that the analogue of Riemann hypothesis for zeta functions of number fields [6], the so called Dedekind zeta functions, holds true. A quantitative version of Artin's primitive root conjecture is proved under GRH by Hooley [9], and unconditionally for all but two unspecified prime roots a by Heath-Brown [8]. The following is a refinement of Artin's primitive root conjecture where in addition the prime m is required to be in a fixed arithmetic progression $1 \pmod{s}$.

Conjecture 2.1. *Let a be a non-zero integer that is not a perfect square nor -1. Let h be the largest integer such that a is an h-th power. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{a})$. Given $s \geq 1$, let $S(a,s)$ be the set of primes $m \equiv 1 \pmod{s}$ such that a is a primitive root modulo m. If both $(s,h) = 1$ and $\Delta \nmid s$, then the set $S(a,s)$ is infinite.*

If $(s,h) > 1$, then the set $S(a,s)$ is finite. Suppose there exists an element m of that set not dividing a. Writing $a = a_0^h$, we have $a^{(m-1)/(s,h)} = a_0^{h(m-1)/(s,h)} \equiv a_0^{m-1} \equiv 1 \pmod{m}$ and so a is not primitive modulo m. Contradiction.

Likewise, if $\Delta \mid s$, the set $S(a,s)$ is finite. By elementary algebraic number theory the smallest m for which $\mathbb{Q}(\sqrt{g}) \subseteq \mathbb{Q}(\zeta_k)$ equals $k = |\Delta|$. The primes $m \equiv 1 \pmod{s}$ split completely in $\mathbb{Q}(\zeta_k)$ and so certainly in the subfield $\mathbb{Q}(\sqrt{a})$. If $m \nmid a$, it then follows that the Legendre symbol $(a/m) = 1$ and so the order of a modulo m is at most $(m-1)/2$, and so $S(a,s)$ is finite.

The conjecture thus claims that if there is no trivial reason for $S(a,s)$ to be finite, it is actually infinite.

Under GRH Lenstra [11, Theorem 8.3] established a far reaching generalization of Artin's original conjecture. In particular, his work implies the truth of Conjecture 2.1. Indeed, under GRH the set $S(a,s)$ has a natural density that can be explicitly given, which was done by Moree [14, Theorem 4]. Combination of the two results yields the following theorem.

Theorem 2.2. *Under GRH Conjecture 2.1 holds true and, moreover, the set $S(m,s)$ has an explicitly determinable density that is a rational multiple times the Artin constant.*

The reader interested in more information regarding the Artin primitive root conjecture and its many generalizations and applications is referred to the survey [15].

2.5. **Asymptotics.** If $\mathcal{C}(n)$ is a family of codes with parameters $[n, k_n, d_n]$ over $\mathbb{F}_q$, the rate R and relative distance δ are defined as

$$R = \limsup_{n\to\infty} \frac{k_n}{n} \text{ and } \delta = \liminf_{n\to\infty} \frac{d_n}{n},$$

respectively. When examining a family of codes, it is natural to ask if this family is asymptotically good or bad in the following sense. A family of code is **asymptotically good** if $R\delta \neq 0$.

Recall the q-ary **entropy function** defined for $0 \leq t \leq \frac{q-1}{q}$ by

$$H_q(t) = \begin{cases} 0, \text{ if } t = 0, \\ t\log_q(q-1) - t\log_q(t) - (1-t)\log_q(1-t), \text{ if } 0 < t \leq \frac{q-1}{q}. \end{cases}$$

This quantity is instrumental in the estimation of the volume of high-dimensional Hamming balls when the base field is $\mathbb{F}_q$. The result we are using in this paper is that the volume of the Hamming ball of radius tn is asymptotically equivalent, up to subexponential terms, to $q^{nH_q(t)}$, when $0 < t < 1$, and n goes to infinity [10, Lemma 2.10.3].

3. Main result

Let s be an integer greater than 1 and $T_{a_1,\ldots,a_{s-1}}$ denote the s-circulant code over $\mathbb{F}_q$ with generator matrix $(1, a_1(x), \ldots, a_{s-1}(x))$ with $a_i(x) \in R_m = \mathbb{F}_q[x]/(x^m - 1)$. Denote by μ_r the **multiplier by** r in R_m, defined for all $f(x) \in R_m$ by $\mu_r(f(x)) = f(x^r)$. (Cf. [10, §4.3]). Note that

$$\mathbb{F}_q G(m,s,r) \simeq \mathbb{F}_q[x,y]/(x^m - 1, y^s - 1, x^r y - yx)$$

as a ring (we are just choosing a special ordering of the elements of $G(m,s,r)$), and the right-hand side is isomorphic to R_m^s as an R_m-module via

$$f_1(x) + f_2(x)y + \ldots + f_s(x)y^{s-1} \mapsto (f_1(x), f_2(x), \ldots, f_s(x)).$$

A construction of metacyclic codes from quasi-cyclic codes similar to the next lemma can be found in [16, Theorem 1].

Lemma 3.1. *If $a_1\mu_r(a_1)\dots\mu_r^{s-1}(a_1) = 1$ and $a_j = a_1\mu_r(a_1)...\mu_r^{j-1}(a_1)$ for all $j \in \{2,\dots,s-1\}$, then $T_{a_1,\dots,a_{s-1}}$ is metacyclic for the group $G(m,s,r)$.*

Proof. Writing an arbitrary codeword as

$$f_1(x) + f_2(x)y + \dots + f_s(x)y^{s-1} \in \mathbb{F}_q[x,y]/(x^m-1, y^s-1, x^ry - yx),$$

we see that left multiplication by y in that ring corresponds to the map

$$(f_1(x),\dots,f_s(x)) \mapsto (\mu_r(f_s(x)), \mu_r(f_1(x)),\dots,\mu_r(f_{s-1}(x)))$$

in R_m^s. For $T_{a_1,\dots,a_{s-1}}$ to be a $G(m,s,r)$-code, it is sufficient to check that it is stable under left multiplication by y (every s-circulant code being clearly stable under left multiplication by x). Reasoning on the generator of $T_{a_1,\dots,a_s}$ the above relation shows that $(\mu_r(a_{s-1}(x)), 1,\dots,$ $\mu_r(a_{s-2}(x)))$ is proportional to $(1, a_1(x),\dots,a_{s-1}(x))$ by an element of R_m. Getting rid of that element between two equations yields the said relations on the elements $a_1(x),\dots,a_{s-1}(x)$. □

Remark 3.2. A natural question is under which conditions $T_{a_1,\dots,a_{s-1}}$ is two-sided, since in this case the code would be abelian [17]. Reasoning in the same way as above on the right multiplication by y and by x we obtain that $T_{a_1,\dots,a_{s-1}}$ is a right ideal in $\mathbb{F}_q[x,y]/(x^m-1, y^s-1, x^ry-yx)$ if and only if $a_{s-1}^s = 1$, $a_j = a_{s-1}^{s-j}$ for all $j \in \{1,\dots,s-2\}$, and $a_j = a_j \cdot x^{jr-1}$ for all $j \in \{1,\dots,s-1\}$. The last condition is equivalent to a_j being constant on the orbits of the $(jr-1)$-th power of the shift, and in the case m is prime and $r \neq 1 \pmod m$, it is easy to see that the set of $T_{a_1,\dots,a_{s-1}}$ satisfying all above conditions is empty: actually $a_1 = a_1 \cdot x^{r-1}$ implies that $a_1 = \lambda(1 + \dots + x^{m-1})$, with $\lambda \in \mathbb{F}_q$. But then

$$a_1\mu_r(a_1)\dots\mu_r^{s-1}(a_1) = \lambda^s(1+\dots+x^{m-1})^s = \lambda^s m^{s-1}(1+\dots+x^{m-1})$$

(the last equality can be proven by induction on $m \geq 2$) cannot be equal to 1.

We now assume that m is a prime, such that q is primitive modulo m. Thus, by the theory of cyclotomic cosets [10, §4.1], we know that $x^m - 1 = (x-1)h(x)$, with h irreducible over $\mathbb{F}_q[x]$.

Lemma 3.3. *Assume that s divides $m-1$ and that the order of r modulo m is s. The number $\Omega_{m,s}$ of the s-circulant codes with the properties in Lemma 3.1 is*

$$\Omega_{m,s} = s' \cdot \frac{q^{m-1}-1}{q^{\frac{m-1}{s}}-1}, \text{ with } s' = (s, q-1).$$

Proof. The CRT for polynomials yields the ring decomposition

$$R_m \simeq \mathbb{F}_q \oplus \mathbb{F}_Q,$$

with $Q = q^{m-1}$.

Write $a_1 = a_1' \oplus \alpha_1, \dots, a_{s-1} = a_{s-1}' \oplus \alpha_{s-1}$, in this decomposition. We study the conditions on $a_1,\dots,a_{s-1}$ given in Lemma 3.1, in the light of this CRT decomposition.

- The conditions on $a_1',\dots,a_{s-1}'$ are $a_1'^s = 1$, and $a_j' = a_1'^{j-1}$ for $j \in \{2,\dots,s-1\}$. The first equation has s' solutions, with $s' = (s, q-1)$ and the rest of a_j is uniquely determined.
- Since, by hypothesis, the order of μ_r is s, the action of μ_r on $\mathbb{F}_Q$, by the characterization of the Galois group of $\mathbb{F}_Q$ is exponentiation by $t = q^{\frac{m-1}{s}}$. The condition on a_1 implies

  $$\alpha_1 \in \{z \in \mathbb{F}_Q \mid z^{1+t+\dots+t^{s-1}} = 1\} = \{A^{t-1} \mid A \in \mathbb{F}_Q^\times\},$$

  a set of size $\frac{t^s-1}{t-1}$. The rest of the α_j's is uniquely determined.

The result follows by multiplying these two independent counts together.

□

The next lemma shows that the codes of Lemma 3.1 have "small" common intersection.

Lemma 3.4. *If $(f_1(x), \ldots, f_s(x)) \in R_m^s$, with a Hamming weight $< m$, then there are at most q codes $T_{a_1,\ldots,a_{s-1}}$ with the properties in Lemma 3.1 such that $(f_1(x), \ldots, f_s(x)) \in T_{a_1,\ldots,a_{s-1}}$.*

Proof. Keep the notation of the proof of Lemma 3.3. Since $a_2, \ldots, a_{s-1}$ are uniquely determined by a_1, we focus on a_1. The Hamming weight condition implies that $f_1(x) \neq 0 \pmod{h(x)}$ (otherwise f_1 would be a nonzero codeword of the repetion code of length m over $\mathbb{F}_q$). Then $a_1(x)$ is uniquely determined modulo $h(x)$ by the equation $f_2(x) \equiv f_1(x)a_1(x) \pmod{h(x)}$. But modulo $x-1$ it can takes q values. The result follows. □

The following results are true under Artin's primitive root conjecture Conjecture 2.1 for the progression $1 \pmod{s}$, which by Theorem 2.2 is guaranteed if GRH holds true.

Theorem 3.5. *Assume Conjecture 2.1 holds true. Let q be a prime and $s > 1$ be an integer such that $q \nmid s$ if $q \equiv 1 \pmod 4$ and $4q \nmid s$ if $q \equiv 3 \pmod 4$ or $q = 2$. For every $0 < \delta < H_q^{-1}(\frac{s-1}{s^2})$, there is a sequence of metacyclic codes over $\mathbb{F}_q$ that are group codes for $G(m, s, r)$ of rate $1/s$ and relative Hamming distance δ.*

Proof. Under these hypotheses on q and s, the existence of infinitely many primes m such that q is primitive modulo m and that s divides $m-1$ is ensured by Artin's primitive root conjecture in arithmetic progression, as shown in §2.4 (for the discriminant of quadratic fields see [18, p.89]). If the number $\Omega_{m,s}$ is strictly larger than q times the size of a Hamming ball of radius $\lfloor \delta ms \rfloor$, then, by Lemma 3.4, there is a code constructed by Lemma 3.1 of minimum distance $> \lfloor \delta ms \rfloor$. This inequality will hold if, using the standard entropic estimates of §2.5, for $m \to \infty$, we have

$$s' \cdot \frac{q^{m-1} - 1}{q^{\frac{m-1}{s}} - 1} > q \cdot q^{msH_q(\delta)},$$

and in particular if $(s-1)/s^2 > H_q(\delta)$. □

We relax the condition that q is prime as follows.

Corollary 3.6. *Assume Conjecture 2.1 holds true. The metacyclic codes over $\mathbb{F}_w$ with $w = q^a$, q a prime and $a \geq 2$, form an asymptotically good family of codes.*

Proof. By the preceding theorem the metacyclic codes over $\mathbb{F}_q$ are asymptotically good. By extension of scalars from $\mathbb{F}_q$ to $\mathbb{F}_w$ (as in [7, Proposition 12]) the result follows. □

The following result was proved for q even by similar techniques, under Artin's conjecture, in [1], and unconditionally in [2] using more advanced probabilistic techniques.

Corollary 3.7. *Assume Conjecture 2.1 holds true. Dihedral codes are asymptotically good in any characteristic.*

Proof. A consequence of Theorem 3.5 and Corollary 3.6 in the case $r = m - 1$ and $s = 2$, for which $G(m, s, r)$ is the dihedral group of order $2m$. □

The following result was proved unconditionally and for all characteristics in [4] using the Bazzi-Mitter approach of [2].

Corollary 3.8. *Assume Conjecture 2.1 holds true. If $p \equiv 3 \pmod 4$, then $G(m, p, r)$-codes over finite fields of characteristic p are asymptotically good.*

Proof. This is a consequence of Theorem 3.5 with $s = q = p$ and of Corollary 3.6 for prime powers. □

4. Conclusion and Open Problem

In this note, we have shown that left ideals in the group ring of a metacyclic group form, for certain values of the parameters, an asymptotically good family of codes. The main open problem would be to extend this result to two-sided ideals. This would allow to show, by the combinatorial equivalence derived in [17], that abelian group codes are asymptotically good. Unfortunately, the conditions obtained in Remark 3.2 seem to suggest that s-circulant metacyclic codes are not the right ones to be considered in this case.

References

[1] A. Alahmadi, F. Özdemir and P. Solé, On self-dual double circulant codes, *Designs, Codes Cryptogr.*, **86**, (2018), 1257–1265.

[2] L.M.J. Bazzi and S.K. Mitter, Some randomized code constructions from group actions, *IEEE Trans. Inform. Theory*, **52**, (2006), 3210–3219.

[3] M. Borello, J. de la Cruz and W. Willems, On checkable codes in group algebras, `https://arxiv.org/pdf/1901.10979.pdf`.

[4] M. Borello and W. Willems, Group codes over fields are asymptotically good, `https://arxiv.org/pdf/1904.10885.pdf`.

[5] Y-L. Cao, Y. Cao, F-W. Fu and J. Gao, On a class of left metacyclic codes, *IEEE Trans. Inform. Theory* **62** (12), (2016), 6786–6799.

[6] H. Davenport,*Multiplicative number theory*, Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

[7] F. Faldum and W. Willems, Codes of small defect, *Des. Codes and Cryptogr.* **10** (1997), 341–350.

[8] D.R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* **37**, (1986), 27–38.

[9] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225**, (1967), 209–220.

[10] W.C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge (2003).

[11] H.W. Lenstra Jr., On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42**, (1977), 201–224.

[12] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Trans. Inform. Theory*, **47** (7), (2001), 2751–2760.

[13] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland (1977).

[14] P. Moree, Uniform distribution of primes having a prescribed primitive root, *Acta Arith.* **89** (1999), 9–21.

[15] P. Moree, Artin's primitive root conjecture – a survey, *Integers* **12A** (2012), No. 6, 1305–1416.

[16] R.E. Sabin, On row-cyclic codes with algebraic structure, *Designs, Codes and Cryptogr.* **4**, (1994), 144–155.

[17] R.E. Sabin and S. Lomonaco, Metacyclic error-correcting codes, AAECC **6**, (1995), 191–210.

[18] P. Samuel, *Théorie algébrique des nombres*, Hermann (1967).