Manuscript submitted to
AIMS' Journals
Volume **X**, Number **0X**, XX **201X**

doi:10.3934/xx.xx.xx.xx

pp. **X–XX**

COMPLEMENTARY DUAL CODES FOR COUNTER-MEASURES TO SIDE-CHANNEL ATTACKS

Claude Carlet

LAGA, UMR 7539, CNRS,
University of Paris VIII and University of Paris XIII,
Department of Mathematics,
2 rue de la liberté, 93 526 Saint-Denis Cedex, France.

Sylvain Guilley

TELECOM-ParisTech, Crypto Group,
37/39 rue Dareau, 75 634 Paris Cedex 13, France;
and Secure-IC S.A.S.,
15 rue Claude Chappe, Bât. B, ZAC des Champs Blancs, 35 510 Cesson-Sévigné, France.

(Communicated by the associate editor name)

Abstract. We recall why linear codes with complementary duals (LCD codes) play a role in counter-measures to passive and active side-channel analyses on embedded cryptosystems. The rate and the minimum distance of such LCD codes must be as large as possible. We recall the known primary construction of such codes with cyclic codes, and investigate other constructions, with expanded Reed-Solomon codes and generalized residue codes, for which we study the idempotents. These constructions do not allow to reach all the desired parameters. We study then those secondary constructions which preserve the LCD property, and we characterize conditions under which codes obtained by direct sum, direct product, puncturing, shortening, extending codes, or obtained by the Plotkin sum, can be LCD.

1. **Introduction.** Codes play a central role in digital communication. Recently, it has been shown that codes can also help improve the security of the information processed by sensitive devices, especially against so-called side-channel attacks (SCA) and fault non-invasive attacks. This paper recalls that linear codes with complementary duals (called LCD), which are linear codes whose intersection with their dual is trivial, play an important role in armoring implementations against these two kinds of non-invasive attacks.

LCD codes, introduced by Massey [20], provide an optimum linear coding solution for the two-user binary adder channel. Some constructions are known: [27, 13, 12]. Some of them are within cyclic codes and in particular quadratic residue (QR) codes. As another example, maximum rank distance (MRD) codes generated by the trace-orthogonal-generator matrices are LCD codes [17]. Asymptotically good LCD codes exist [23].

2010 *Mathematics Subject Classification.* Primary: 94B15, 94B65; Secondary: 14G50.

Key words and phrases. Side-channel analysis, fault injection analysis, hardware trojan horses, linear codes with complementary duals (LCD), cyclic codes, Bose, Ray-Chaudhuri and Hocquenghem (BCH) codes, generalized residue codes.

However, SCA sheds a new light on LCD codes and poses more accurately the question of their effective construction achieving good minimum distance, especially in the context of large rate.

QR codes are not well adapted to this context and we explore generalized residue codes (GRC), candidates for being LCD and for which theoretical results exist regarding their minimum distance [7]. However, in practically relevant cases, the results about minimum distances are void. Therefore, we complement the state-of-the-art of GRC, with the viewpoint of their construction and of the need for a lower bound on their minimum distance. We also introduce a way of constructing LCD codes by expanding Reed-Solomon codes. Finally, we study secondary constructions of LCD codes, which help reaching the exact parameters needed in our framework.

2. **Motivation.**

Implementations of cryptographic algorithms are prone to SCA and fault attacks that aim at extracting the secret key when the algorithm is running over some device. Non-invasive attacks observe some leakage (such as electromagnetic emanations) or perturb internal data (for example with electromagnetic impulses), without damaging the system. They are a special concern insofar as they leave no evidence that they have been perpetrated. Those attacks can be classified into two categories:

- Side-channel attacks (SCA), which consist in passively recording some leakage, that is the source of information to retrieve the key;
- Fault injection attacks (FIA), which consist in actively perturbing the computation so as to obtain exploitable differences at the output.

Few generic protections, demonstrably provable against both threats, have been proposed. The best understood and most studied protection against SCA is achieved with masking. Every sensitive data x, say a binary vector, employed in the cryptographic algorithm is exclusived-or with one uniformly distributed random vector of the same length, called mask. We are interested in this article in a *homomorphic* computation. This means that the computations are carried out on the masked data itself. Therefore, it must be possible, from a masked sensitive variable, denoted by z, to recover x (e.g., for the final demasking at the end of the computation). This is possible if the sensitive data and the masks belong to two supplementary subspaces of a larger space vector. Indeed, by definition of supplementary subspaces, any element of the large space vector decomposes itself in a unique way as the sum of two elements (in Boolean vector spaces, the sum is the exclusive-or, denoted by "+" in the sequel). It is thus decided to interpret those two elements as the sensitive data and the mask. This method is called *Orthogonal Direct Sum Masking* (ODSM), see [8].

We call n the dimension of this large vector space, which practically is $\mathbb{F}_2^n$. Now, we call C and D the two supplementary vector spaces:

$$\mathbb{F}_2^n = C \oplus D \ . \tag{1}$$

The masks are the codewords of code D. By the rank-nullity theorem, if the dimension of C is k, then the dimension of D is $n-k$. Let us consider generator matrices G and G' of C and D, respectively. Then every vector $z \in \mathbb{F}_2^n$ can be written in a unique way as $z = xG + yG'$, $x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^{n-k}$. If C and D are furthermore

orthogonal with respect to the usual inner product, i.e., $D = C^\perp$, then C is said complementary dual[1].

Definition 2.1. A *linear* code C is called *complementary dual* (LCD) if C and $C^\perp$ are supplementary, that is (given their dimensions), $C \cap C^\perp = \{0\}$.

Remark 1. *Let C be a linear code. The space vector $C \cap C^\perp$ is called the* hull *of C. So, C is LCD if and only if its hull has a zero dimension.*

Note that $D = C^\perp$ if and only if G' is a parity-check matrix of C, that is, $GG'^{\mathsf{T}} = 0$, where G'^{T} is the transposed matrix of matrix G'; we denote then G' by H. We can use an orthogonal projection to recover x and y from z: the relation $z = xG + yH$ implies $zH^{\mathsf{T}} = yHH^{\mathsf{T}}$ and $zG^{\mathsf{T}} = xGG^{\mathsf{T}}$. The next characterization is due to Massey [20]:

Proposition 1. *Let C be a linear code. Let G be a generator matrix of C and H a parity-check matrix. Then the three following properties are equivalent:*

1. *C is LCD,*
2. *the matrix HH^{T} is invertible,*
3. *the matrix GG^{T} is invertible.*

We deduce from $zH^{\mathsf{T}} = yHH^{\mathsf{T}}$ and $zG^{\mathsf{T}} = xGG^{\mathsf{T}}$, and from Proposition 1 that if C is LCD, the matrices of the two projections $z = xG + yH \mapsto x$ and $z \mapsto y$ are respectively (see also [20, Proposition 1]):

$$G^{\mathsf{T}}(GG^{\mathsf{T}})^{-1} \text{ so that } x = zG^{\mathsf{T}}(GG^{\mathsf{T}})^{-1} \ , \tag{2}$$

$$H^{\mathsf{T}}(HH^{\mathsf{T}})^{-1} \text{ so that } y = zH^{\mathsf{T}}(HH^{\mathsf{T}})^{-1} \ . \tag{3}$$

Note that, $G^{\mathsf{T}}(GG^{\mathsf{T}})^{-1}$ is also known as the pseudo-inverse (or Moore-Penrose inverse [1]) G^+ of G.

The quality of the masking is an important factor. Let $\phi : \mathbb{F}_2^n \to \mathbb{R}$ be a leakage function, that describes how z is leaked outside of device. The masked word z conceals the information x at *first degree* if for all pseudo-Boolean function $\phi : \mathbb{F}_2^n \to \mathbb{R}$ of unitary numerical degree [9, Sec. 2.1], all the averages of $\phi(z)$ over the masks $d \in D$ for a given x are equal irrespective of x. Indeed, first-degree attacks consist in correlating the measured leakage with a leakage model, the latter being precisely independent of x, since equal to the expectation of $\phi(z)$ knowing x [22]. This means that $\forall x \in \mathbb{F}_2^k, \sum_{y\in\mathbb{F}^{n-k}} \phi(xG + yH)$ are the same, i.e., equal to $\sum_{y\in\mathbb{F}^{n-k}} \phi(yH)$ (for $x = 0$). Now, this notion can be generalized (see [3, Def. 2]). A zero-offset masking countermeasure is of *degree at least* d if $\forall x \in \mathbb{F}_2^k, \sum_{y\in\mathbb{F}^{n-k}} \phi(xG + yH) = \sum_{y\in\mathbb{F}^{n-k}} \phi(yH)$ for all ϕ of numerical degree at most d. The greater the degree of the countermeasure, the harder to pass a successful SCA. Actually, it is known from [8, Proposition 3] that the countermeasure is $(d-1)$-th degree secure if D has dual distance d, i.e., if C has minimum distance d. This result has been independently validated in [15] for $d \in \{1, 2\}$. This characterization is equivalent to the $(d-1)$-th order *probing security*, since any tuple of $(d-1)$ bits of the mask is uniform random, hence perfectly conceals the $(d-1)$ information bits.

Let us now consider a fault injection attack (FIA). The state z is modified into $z + \varepsilon$, for some random $\varepsilon \in \mathbb{F}_2^n$. By supplementarity of C and D, there exists a unique ordered pair $(e, f) \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$ such that $\varepsilon = eG + fH$. A detection strategy

[1] "supplementary" would seem a more appropriate term than "complementary", but the terminology being more than ten year old, we must keep it as is.

could consist in decoding z into (x, y), and checking that we recover the genuine values unchanged. However, x is sensitive: the purpose of the protection is exactly to avoid representing x by replacing it by z. The random variable y, from its side, does not convey any (statistically) exploitable information. So, checking whether or not the mask has been altered, i.e., $zH^{\mathsf{T}}(HH^{\mathsf{T}})^{-1} \stackrel{?}{=} y$, is a harmless detection strategy. This happens if and only if $f = 0$, i.e., $\varepsilon \in C$. As $\varepsilon = 0$ is pointless (since without observable effect), harmful faults only happen if $\varepsilon \in C \setminus \{0\}$. In particular, the Hamming weight of ε must be greater or equal to the minimum distance d of code C for the fault not to be detected. Now, given that the minimum distance d of C is a design parameter, it is set as high as possible.

Therefore, have C be LCD of greatest possible minimum distance simultaneously improves the resistance against SCA and FIA.

There are two kinds of designs that can benefit from the described protection. The first one is the implementation of hardware accelerators for block ciphers, such as the AES. In this case, the data to protect are typically bytes, with $k = 8$ (see for instance this case study [8]). It is shown that an optimal linear code of parameters $[16, 8, 5]$ is LCD, and is very suitable for embedded devices, as the length $n = 2k = 16$ consists in one word (two bytes). Besides, it happens that the $[16, 8, 5]$ code is *unique*, as proven by Betsumiya and Harada in [2, Corollary 6, page 19]. Remarkably, this code is not only **LCD**, but also **CIS** (i.e., with Complementary Information Sets) [11, Sec. V.A, page 6004] while being **odd formally self-dual**. The second kind is a general-purpose processor executing software cryptography (see for instance [6], where a tiny processor is protected). Its registers can be protected individually (hence $k = 8, 16, 32$). For an improved security, it can be advantageous to mask all the registers seen as one unique resource, made up of a few hundreds to a few thousands bits. Therefore, we are interested in codes of various dimensions, ranging from $k = 8$ to $k \approx 4096$.

Side-channel analysis starts to be difficult even at low degrees (e.g., d is equal to a few units, such as $d = 2, 3, 4$). The same applies to perturbation attacks: if all faults on $d = 1, 2, 3, 4$ bits are detected, then the success of FIA is compromised. Now, *hardware trojan horses* (HTHs) make up a special threat. HTHs are gates added by an adversary (e.g., a silicon foundry) into the design at fabrication time. Those gates allow to deliver a malicious payload on a crafted activation condition. The activation results from a triggering, decided based on the value of some bits of the circuit. Thus, in a circuit protected by a LCD code C of minimum distance d, the HTH must connect to at least d bits to receive enough bits for a partial demasking of the state. Symmetrically, the payload is delivered by altering some bits of the circuit. Consequently, the HTH must modify at least d bits to bypass an integrity check. Therefore, in order to preventively refrain the insertion of HTH trigger logic and in order to proactively detect the effect of the HTH payload, the minimum distance d of LCD codes must be set has high as possible (refer to [6] for more details). Now, it is known that for too large a value of d (e.g., $d > 16$), then the added gates making up the HTH will be so numerous that the HTH will be trivially disclosed, e.g., by some visual inspection [5].

The problem is thus the following: for a given dimension k (architecture parameter) and minimum distance d (security parameter), find a LCD code of length n as small as possible (and therefore, of *rate* k/n as large as possible).

Remark 2 (More general formalization)**.** *Let us consider two codes C and D which are supplementary in $\mathbb{F}_q^n$, where q is a prime power (e.g., 2), but not necessarily dual. We denote by d the minimum distance of C and by d' the dual distance of D. Then the researched compromise is between* $\min(d, d')$ *and the dimension of code C. Indeed, if C is a subcode of C_1 and D is a supercode of D_1, then $d \geq d_1$ and $d' \geq d'_1$ (since $D^\perp$ is a subcode of $D_1^\perp$), which implies that* $\min(d, d') \geq \min(d_1, d'_1)$.

An application of remark 2 can be found in [4, 10]. The context is that of an asymmetrical defense against HTH: the HTH must connect to at least d' bits to be able to trigger itself, and must modify at least d bits to be able to deliver its payload.

In the sequel, we will consider only LCD codes, for which $C = D^\perp$ hence $d = d'$.

The rest of the paper is organized as follows.

- Sec. 3 gives several constructions of codes, which make up the bulk of the countermeasures.
- Sec. 4 gives constructions from other codes, thereby allowing for optimizations. Especially, puncturing, shortening and extending allows to fine-tune a code that has the almost expected security level. Typically, it can be beneficial to start from a code whose dimension is little larger than the target dimension, in which case it can be shortened. This is beneficial as both the dimension and the length are decremented, which allows to reduce the cost of the implementation while at the same time have a code that better fits the intended dimension.

3. **Constructions.** In this section we study, with a practical viewpoint, how the known primary constructions[2] can allow to obtain effective LCD binary codes with large minimum distance and large rate. An important selection criterion is the existence of a bound on the minimum distance, that otherwise cannot be computed by testing all the possible Hamming weights of nonzero codewords since our codes can have lengths of the order of one or several thousands.

LCD cyclic codes, which have a minoration on their minimum distance via the BCH bound, have been characterized in [27]. The condition for being LCD is rather simple and not difficult to achieve. Moreover, a potentially stronger lower bound on the minimum distance exists for the sub-class of quadratic-residue (QR) codes, which can also be LCD. A QR code has for length a prime number n and has a minimum distance d at least $\sqrt{n}$. A binary QR code has length congruent with ± 1 modulo 8 and is LCD if the length is congruent with 1 modulo 8 [19, Chp. 16, §6, page 495]. Asymptotically, $\sqrt{n}$ is a rather low value compared with the Gilbert Varshamov bound, but such value is not far from what we need in our framework. The main drawback of QR codes is that their dimension equals $\frac{n\pm 1}{2}$ (namely $\frac{n+1}{2}$ if we exclude 1 as possible zero of QR codes, and $\frac{n-1}{2}$ otherwise), while we need larger dimensions. Indeed, given the dimension k (which can be of the order of one or several thousands) and some number δ (say, at most 64), we look for a LCD code of length n as small as possible such that $d \geq \delta$. This leads us to consider (in Sec. 3.3) a generalization of QR codes whose lengths are not prime.

We first recall in Sec. 3.1 the definition and some properties of cyclic codes in general, and of LCD cyclic codes in particular. We then prove in Sec. 3.2 that there

[2]By that, we mean constructions from scratch. We shall deal with secondary constructions, which deduce LCD codes from other codes, in the next section.

exist LCD Reed-Solomon codes of any dimension over $\mathbb{F}_{q^m}$; but their length can hardly be controlled. Thus, we define in Sec. 3.3 the generalized residue codes[3] and study LCD codes within them.

3.1. **LCD cyclic codes.** In all this paper, q is a prime power; for applications against SCA, FIA, and HTH, q shall be considered to be a power of 2.

Definition 3.1 (Cyclic code)**.** A linear code C of length n over a finite field $\mathbb{F}_q$ is cyclic if it is stable by any circular rotation.

We shall always consider n co-prime with q. The codewords can also be represented as polynomials in the algebra $A = \mathbb{F}_q[X]/(X^n - 1)$. In this representation, a code is cyclic if and only if it is an ideal of A. A cyclic code $C \neq \{0\}$ is generated by the (unique) normalized nonzero polynomial $g(X)$ of the smallest degree in C, which is always a divisor of $X^n - 1$ (conversely, any divisor of $X^n - 1$ is the generator polynomial of a cyclic code of length n). The zeros of $g(X)$ in the extension of $\mathbb{F}_q$ equal to $\mathbb{F}_{q^m}$ where m is the multiplicative order of q modulo n (i.e., the smallest positive integer such that n divides $q^m - 1$) are then n-th roots of unity. They are called the zeros of the code. The other n-th roots of unity are called the non-zeros of C. Since n is co-prime with q, the zeros of $X^n - 1$ and then of $g(X)$ are simple. This is because the derivative nX^{n-1} of $X^n - 1$ has 0 for unique zero. The dimension of the code equals the number of its non-zeros because every codeword is in fact a multiple of degree at most $n - 1$ of $g(X)$ in $\mathbb{F}_q[X]$. The set of zeros is stable under the Frobenius automorphism $\gamma \mapsto \gamma^q$. Conversely, any set of n-th roots of unity stable under the Frobenius automorphism is the set of zeros of a cyclic code over $\mathbb{F}_q$. Let β be a primitive n-th root of unity. Let C be a cyclic code of zeros $\{\beta^j,\, j \in J \subseteq \mathbb{Z}/n\mathbb{Z}\}$. The BCH bound states that the minimum distance of C is bounded below by the length of any string of consecutive elements in J, plus 1. The dual $C^\perp$ is the cyclic code whose zeros are the inverses of the non-zeros of C [19, Chap. 7, page 188] and $C \cap C^\perp$ is the cyclic code whose set of zeros equals the union of the zeros of C and those of $C^\perp$. It equals $\{0\}$ if and only if this union equals the set of all n-th roots of unity. Hence:

Proposition 2. [27, Theorem at page 392] *A cyclic code C is LCD if and only if its set of zeros is stable by the multiplicative inverse, i.e., if and only if its generator polynomial $g(X)$ is self-reciprocal.*

Example 1. The binary cyclic code of length 17 whose zeros are

$$\{\beta^j,\, j = 0, 1, 2, 4, 8, 9, 13, 15, 16\}$$

is LCD and has parameters $[17, 8, 6]$, and its generator polynomial is $X^9 + X^6 + X^5 + X^4 + X^3 + 1$. Note that the set of zeros is stable under the Frobenius $\gamma \mapsto \gamma^2$, which makes the code binary, and that the string $15, 16, 0, 1, 2$ in $\mathbb{Z}/17\mathbb{Z}$ has length 5; the BCH bound is then tight for this code.

3.2. **Expanded LCD Reed-Solomon codes.** According to Proposition 2, those Reed-Solomon codes whose sets of zeroes are stable under inversion are LCD codes. These codes provide full choice of the dimension (see the proof of Lemma 3.2 below), but not of the length, which must be primitive. Being MDS, they have optimal

[3] Earlier works, such as [25, 26] generalized QR codes to *prime power* (instead of *prime*) lengths and to *t-th order residues* (instead of *quadratic*). Our work goes beyond insofar as we consider any length co-prime with the field characteristic q (for our application, $q = 2$).

minimum distance. But they are not binary and are then less useful for the applications described in introduction. However, there exists a way of transforming them into binary LCD codes. Mapping a code C over $\mathbb{F}_{q^m}$ onto a code C' over $\mathbb{F}_q$ by replacing each coordinate by the binary vector of its coordinates relative to a fixed basis is called *expanding* the code. For doing so, we can use that $\mathbb{F}_{q^m}$ is a field extension of $\mathbb{F}_q$, and given an irreducible polynomial P over $\mathbb{F}_q$ and denoting each element $a \in \mathbb{F}_{q^m}$ as $\sum_{i=0}^{m-1} a_i X^i \ [\mod P(X)]$, replace a by $(a_0, \ldots, a_{m-1})$. Under the computer algebra system Magma, P is `DefiningPolynomial`$(\mathbb{F}_{q^m})$ and C' is `SubfieldRepresentationCode`(C). If C has parameters $[n, k, d]_{q^m}$, then C' has parameters $[mn, mk, d']_q$, where $d' \geq d$.

According to [21, Theorem 5.1.18 page 103], there exists a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if either q is even or both q and m are odd. In the application against attacks (Sec. 2), $q = 2$ and we can then consider a self-dual basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. We have the simple observations:

Proposition 3. *If a code over $\mathbb{F}_{q^m}$ is LCD, then the expanded code relative to a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is also LCD.*

Proof. Let $(\alpha_1, \ldots, \alpha_m)$ be a self-dual basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is such that $\mathrm{tr}(\alpha_i \alpha_j) = 1$ if $i = j$ and 0 otherwise, where "tr" is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Then the vector $\bar{x}$ of the coordinates of x relative to this basis is $(\mathrm{tr}(\alpha_1 x), \ldots, \mathrm{tr}(\alpha_m x))$. For all $x, y \in \mathbb{F}_{q^m}$, we have $\mathrm{tr}(xy) = \mathrm{tr}((\sum_{i=1}^m \alpha_i \mathrm{tr}(\alpha_i x))(\sum_{j=1}^m \alpha_j \mathrm{tr}(\alpha_j y))) = \sum_{i=1}^m \mathrm{tr}(\alpha_i x)\mathrm{tr}(\alpha_i y) = \bar{x} \cdot \bar{y}$. Orthogonality in $\mathbb{F}_{q^m}$ and in the expanded version $\mathbb{F}_q^m$ being equivalent, the expanded code C' of C satisfies ${C^\perp}' = {C'}^\perp$, for all linear code C on $\mathbb{F}_{q^m}$. □

Lemma 3.2. *For all primitive length $n = q^m - 1$ and all $0 < k < q^m$, there exists an expanded LCD Reed-Solomon code of parameters $[nm, km, d]$ with $d \geq n - k + 1$.*

Proof. Let β be a primitive element of $\mathbb{F}_{q^m}$. For any integer b, the code generated by the polynomial $g_b(X) = \prod_{j=0}^{n-k-1}(X - \beta^{j+b})$ is a Reed-Solomon code of parameters $[n = q^m - 1, k, d = n - k + 1]_{q^m}$. If k is odd, then the polynomial $g_{(k+1)/2}(X)$ is self-reciprocal, because its set of (simple) zeros, $\{\beta^j, (k+1)/2 \leq j \leq n - (k+1)/2\}$, is stable by inversion. If k is even, then $g_{-(n-k-1)/2}(X)$ is self-reciprocal, because its set of (simple) zeros, $\{\beta^j, |j| \leq (n-k-1)/2\}$, contains 1 and is stable by inversion. So, irrespective of the parity of k, there exists a Reed-Solomon code generated by a self-reciprocal polynomial, and by Proposition 2, this code is LCD. We apply then Proposition 3. □

Example 2 (Application of Lemma 3.2)**.** By choosing $q = 2$, $m = 10$ and $k = 644$, we can build the LCD Reed-Solomon code of generating polynomial $g_{-(n-k-1)/2}(X) = \prod_{j=-189}^{+189}(X - \beta^j)$, where β is a primitive element of $\mathbb{F}_{1024}$. Its parameters are $[1023, 644, 380]_{1024}$. Its *expanded* code (i.e., its representation in $\mathbb{F}_2$) is also a cyclic LCD code (by Proposition 3), and has parameters $[10230, 6440, d]_2$ with $d \geq 380$.

The length $(q^m - 1)m$ quickly explodes (for $q = 2$, it is respectively equal to 1, 6, 21, 60, 155, 378, 889, 2040, 4599, 10230 for $1 \leq m \leq 10$). We need to investigate more constructions.

3.3. **LCD generalized residue codes.** Let n be any integer co-prime with a prime power q and let t be any positive integer. Let Q be the set of t-th powers in

$\mathbb{Z}/n\mathbb{Z}$:

$$Q = \{i^t,\, i \in \mathbb{Z}/n\mathbb{Z}\} \subseteq \mathbb{Z}/n\mathbb{Z}\ .$$

Then Q is stable under multiplication in the sense that, for any $s \in Q$, the mapping $r \in Q \mapsto sr$ is valued in Q (indeed, for every $i^t, j^t \in Q$, we have $i^t j^t = (ij)^t$). Note that, since n is not assumed to be a prime, the image set of such mapping may be strictly included in Q (for the same reason, we do not exclude $i = 0$ in the definition of Q above since there can exist 0 divisors) and $\mathbb{Z}/n\mathbb{Z} \setminus Q$ may not be stable under all such mappings. Assume that q belongs to Q. Then Q is stable under multiplication by q, in the strong sense that the mapping $r \in Q \mapsto qr$ has image set Q, since q being co-prime with n, the multiplication by q is a permutation of $\mathbb{Z}/n\mathbb{Z}$, and $Q^* = Q \setminus \{0\}$ is also stable under multiplication by q.

Proposition 4. *Let n be an odd positive integer and t be any positive integer. Let Q be the set of t-th powers in $\mathbb{Z}/n\mathbb{Z}$. Assume that q and -1 both belong to Q. Then the cyclic code C of length n whose zeros are β^i, $i \in Q$ (resp. $i \in Q^*$, $i \in \mathbb{Z}/n\mathbb{Z} \setminus Q$, $i \in \mathbb{Z}/n\mathbb{Z} \setminus Q^*$) where β is a primitive n-th root of unity in an extension field of $\mathbb{F}_q$, is a cyclic LCD code.*

Proof. C is q-ary since its set of zeros is stable under the Frobenius automorphism, and Q being stable under multiplication by -1 in $\mathbb{Z}/n\mathbb{Z}$, C is LCD. □

Note that, given t, it is easy to find integers n such that q and -1 are in Q: it is enough to take n as a common divisor of an integer of the form $r^t - q$ and of an integer of the form $s^t + 1$.
But since n is not assumed to be a prime, the size of Q may be strictly smaller than $1 + \frac{n-1}{\gcd(t,n-1)}$ (that is, $\frac{n+1}{2}$ if $t = 2$ and n is odd) and the dimension $k = n - \mathsf{card}(Q)$ of the code may be larger than $(n-1)(1 - \frac{1}{\gcd(t,n-1)})$ (that is, $\frac{n-1}{2}$ if $t = 2$ and n is odd).

We give in Table 1 the values of $n \leq 10,000$ such that $q = 2$ and -1 are quadratic residues ($t = 2$) and Q has size strictly smaller than $\frac{n+1}{2}$. They are not numerous but they exist. We observe that $\mathsf{card}(Q)$ either is near $\frac{n}{2}$ or is near $\frac{n}{4}$ (which is of course more interesting for us since it gives a larger dimension). Note that the only way we know of bounding below the minimum distance is then by using the BCH bound.

Remark 3. *For classical QR codes, n is a prime number (and $\mathbb{Z}/n\mathbb{Z}$ is then a field) and $t = 2$. Given a nonzero codeword $f(X)$ of minimum weight d in the code C of zeros β^i, $i \in Q^*$, and j a non-residue, the polynomial $f(X^j)$ is a nonzero codeword in the code of zeros β^i, $i \in \mathbb{Z}/n\mathbb{Z} \setminus Q$, and $f(X)f(X^j)$ belongs then to the intersection of these two codes and is a multiple of $\sum_{i=0}^{n-1} X^i$ which has weight n. Then $d^2 \geq n$ (but since the size of Q^* equals $\frac{n-1}{2}$, the dimension of the code is $\frac{n\pm1}{2}$, which is too small for our purpose). We need then to generalize.*

Proposition 5. *Let n be a prime number co-prime with q (i.e. not dividing q) and t be any integer. Let $e = \gcd(n-1, t)$ and Q be the set of t-th powers in $\mathbb{Z}/n\mathbb{Z}$. Assume that q and -1 both belong to Q. Then the binary LCD code of Proposition 4 has rate $\frac{n - \frac{n-1}{e}}{n} = \frac{e - 1 + \frac{1}{n}}{e}$ and minimum distance d satisfying $d^e \geq n$.*

Proof. Let α be a primitive element of the field $\mathbb{Z}/n\mathbb{Z}$; we have $Q^* = \{\alpha^{je},\, j \in \mathbb{Z}/(n-1)\mathbb{Z}\}$ and $(\mathbb{Z}/n\mathbb{Z})^* = \bigcup_{i=0}^{e-1} \alpha^i Q^*$. Then, since $f(X^{\alpha^{-i}}) = 0$ if and only if $X^{\alpha^{-i}} \in \{\beta^j,\, j \in Q^*\}$, that is, $X \in \{\beta^{\alpha^i j},\, j \in Q^*\}$, if $f(X) \in C$ the polynomial

$\prod_{i=0}^{e-1} f(X^{\alpha^{-i}})$ has any element β^j, $j \in (\mathbb{Z}/n\mathbb{Z})^*$ for zero and is then a multiple of $\sum_{i=0}^{n-1} X^i$. This completes the proof since $w_H(\prod_{i=0}^{e-1} f(X^{\alpha^{-i}})) \leq (w_H(f))^e$. □

We have then a trade-off between minimum distance and rate.

Remark 4. *The article* [7] *also introduces* generalized residue codes. *Moreover, this article provides an lower bound on the minimum distance of such codes. However, in our context of LCD codes, this bound is not exploitable. For instance, the first entry in Table 1 of rate close to* 3/4 *(and not only* 1/2*) has length* $n = 697$. *For this length, we have the decomposition* $X^{697} - 1 = (X - 1)P(X)\Phi_n(X)$, *where (using notations borrowed from* [7]*):*

- $\Phi_n(X)$ *is a product of* 16 *irreducible polynomials of degree* 40, *and*
- $P(X)$ *is a polynomial of degree* 56, *which decomposes into* 2 *irreducible polynomials of degree* 8 *and* 2 *irreducible polynomials of degree* 20.

Thus, according to [7, Theorem 3], *the lower bound on* d, *the minimum distance of the code, is:* $56d^{16} \geq 697$, *which does not give any information on* d *because this inequation is true for all* $d > 1$.

Remark 5. *The paper* [18] *also introduces a bound for minimal distances on generalized residue codes. However, for meaningful examples, it degenerates to* $d^t \geq n' = 1$, *which does not learn anything on* d *(at least for the examples given in* [18]*).*

3.4. **Generating the codes by the use of idempotents.** The generator polynomial of a cyclic code C of length n may be complex to calculate, because this needs to calculate in the Galois extension of $\mathbb{F}_q$ containing a primitive n-th root of unity β. An alternative way is to use an idempotent as generator of the code (this method is well-known and specially simple for classical quadratic residue codes, see [19, Chap. 16, §3, page 484]). Let $g(X)$ be the generator polynomial of a cyclic code C. We have $X^n - 1 = g(X)h(X)$ where $h(X)$ is co-prime with $g(X)$ since n is odd (all zeros of $X^n - 1$ being then simple). Bezout's theorem implies then the existence of two polynomials $u(X), v(X)$ such that $g(X)u(X) + h(X)v(X) = 1$, which implies $(g(X)u(X))^2 = g(X)u(X) \pmod{X^n - 1}$. Then $E(X) = g(X)u(X)$ is an idempotent in $\mathbb{F}_q[X]/(X^n - 1)$. Moreover, $g(X) = (E(X) + h(X)v(X))g(X) = E(X)g(X) \pmod{X^n - 1}$ implies that $E(X)$ is also a generator of C. Using that $E(X)$ is an idempotent, we have that $f(X) \in C$ if and only if $f(X)E(X) = f(X)$. This implies that $E(X)$ is unique, since if another idempotent $F(X)$ exists in C, we have $F(X)E(X) = F(X) = E(X)$. Note that E applied to n-th roots of unity takes values in $\mathbb{F}_2$ (this is in fact a necessary and sufficient condition for $E(X) \in C$ to be an idempotent [19, Chap. 16, §3, Theorem 2 at page 484]).

Proposition 6. *Let* C *be a cyclic code over* $\mathbb{F}_q$. *Let* $E(X)$ *be the idempotent of* C. *Then* C *is LCD if and only if* $E(X)$ *is self-reciprocal, that is, if and only if the idempotent associated to* $C^\perp$ *is* $1 - E(X)$.

Proof. If C is LCD, then $g(X)$ and $h(X)$ are self-reciprocal, and $E(X)$ which is obtained from $g(X)$ and $h(X)$ by the extended Euclidean algorithm, is self-reciprocal as well. Conversely, if $E(X)$ is self-reciprocal, then the zeros of the code, which are the common zeros of $E(X)$ and $X^n - 1$, are globally stable under inversion and C is LCD. The idempotent of $C^\perp$ equals the reciprocal of $1 - E(X)$, since $1 - E(X)$ is an idempotent (note that $(1 - E(X))^2 = 1 - 2E(X) + (E(X))^2 = 1 - E(X)$) whose common zeros with $X^n - 1$ equal the non-zeros of the code. □

Case of generalized residue codes for $q = 2$:

Proposition 7. *Let n be an odd positive integer and t be any positive integer. Let Q be the set of t-th powers in $\mathbb{Z}/n\mathbb{Z}$. Assume that $q = 2$ belongs to Q. Let C be the binary cyclic code of length n over $\mathbb{F}_q$ whose zeros are β^i, $i \in Q^*$ where β is a primitive n-th root of unity in an extension field of $\mathbb{F}_q$. Let $P(X) = \sum_{j\in Q} X^j$. If every nonzero element in Q is co-prime with n, then the idempotent of code C is $P(X)$ or $1 + P(X)$.*

Proof. Since $2 \in Q$, $P(X)$ satisfies $P^2(X) = \sum_{j\in Q} X^{2j} \equiv P(X) \pmod{X^n - 1}$ and is then an idempotent. For every t-th power residue r, we have $P(\beta^r) = \sum_{j\in Q} \beta^{rj}$, and if r is co-prime with n then we deduce that $P(\beta^r) = \sum_{j\in Q} \beta^j = P(\beta) \in \mathbb{F}_2$. □

Note that adding $\beta^0 = 1$ to the zeros of the code (resp. withdrawing β^0 if it was a zero) corresponds to multiplying (resp. dividing) the generator polynomial by $(X + 1)$. The idempotent becomes $E(X) + \frac{X^n+1}{X+1}$ since the idempotent element $\frac{X^n+1}{X+1}$ of the algebra A takes value 1 at 1 and value 0 at any other n-th root of unity.

3.5. **When the length n is a prime power.** We have now a simple way to practically generate LCD generalized residue codes. But we need to check that the conditions "$q \in Q$", "$-1 \in Q$" and "every nonzero element in Q is co-prime with n" can be satisfied simultaneously. Of course if n is a prime, the last condition is satisfied. If $t = 2$ (which, as we saw above, can give good rates for some values of n which are not primes) and n is the square of a prime, we have:

Proposition 8. *Let p be any prime number and $n = p^r$ for some $r \geq 1$. Let $Q = \{i^t, i \in \mathbb{Z}/n\mathbb{Z}\}$ where $t \geq r$. Then every nonzero element in Q is co-prime with n.*

Proof. Indeed, let $0 < i = kp + l < n$, with $l < p$. Then $i^t \equiv l^t \pmod{p}$ and if $i^t \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$ then $l \neq 0$ and i^t is then co-prime with p and then with n. □

We give in Table 2 the first values of p and $n = p^2$ such that $q = 2$ and -1 are quadratic residues (note that all these values of p are congruent with 1 mod 8 since if 2 and -1 are quadratic residues mod p^2 they are also quadratic residues mod p and we know from [19, Chap. 16, §6, page 495] that p is then congruent with 1 mod 8) and the corresponding values of the size of Q. We observe that this size is smaller than $\frac{n+1}{2}$ which is easily proved in general since two elements $i = kp + l$ and $i' = k'p + l'$ of $\mathbb{Z}/n\mathbb{Z}$ have the same square if and only if $p|(l'^2 - l^2)$, that is, $l = l'$ or $l' = p - l$, and in the case $l = l'$, then $k = k'$ (since $p|k' - k$), and in the case $l' = p - l$, then $k' = k - \frac{p+1}{2}$.

We can now generalize Proposition 5 to the case where n is not prime, but a power of a prime. Notice that Ling and Xing [18], and also Sharma, Bakshi and Raka [24], study generalized residue codes. However, the minimum distances given in [18, Sec. V, page 204] and [24, Table 1, page 1083] have been computed thanks to Magma, and does not result from a mathematical result. We provide this proposition:

Proposition 9. *Let $n = p^r$, where p is a prime and $r \geq 1$, and let $t \geq r$. Let $e = \gcd(p^{r-1}(p-1), t)$ and Q be the set of t-th powers in $\mathbb{Z}/n\mathbb{Z}$. Assume that q and -1 both belong to Q. Then the q-ary LCD code C of Proposition 4 (with zeros in Q^*) has rate $\frac{e-1+\frac{1}{p}}{e}$ and minimum distance d satisfying $d^e \geq p$.*

Proof. The non invertible elements of $\mathbb{Z}/n\mathbb{Z}$ are the multiples of p, and the group (say G) of invertible elements (the unities) is cyclic of order $p^k - p^{k-1} = p^{k-1}(p-1)$ and of generator $g = a(p+1)$, where a is an element of order $p-1$. Indeed, we have $(p+1)^{p^k} = p^{k+1}q_k+1$ where q_k is coprime with p, and this implies that $p+1$ has order p^{r-1}. If we take $t \geq r$, then the t-th power of any non-invertible element is equal to 0 (note that this reduces the size of Q and thus increases the rate) and Q^* is the cyclic group of unities generated by g^t. Let us denote $e = \gcd(p^{r-1}(p-1), t)$. The group Q^* has order $\frac{p^{r-1}(p-1)}{e}$, and G equals the union $\bigcup_{i=0}^{e-1} g^i Q^*$. Let $f(X) \in C$. Then $\prod_{i=0}^{e-1} f(X^{g^{-i}})$ equals $\frac{X^n+1}{P(X)}$ where $P(X) = \prod_{j=0}^{p^{r-1}-1}(X + \beta^{pj})$. The β^{pj} being all (n/p)-th roots of the unity, we have $P(X) = X^{n/p} + 1$. Hence $\frac{X^n+1}{P(X)}$ has weight p and we have $d^e \geq p$. Finally, the rate is $\frac{p^r - \frac{p^{r-1}(p-1)}{e}}{p^r} = \frac{e-1+\frac{1}{p}}{e}$. □

Remark 6. *The bound on d given in Proposition 5 is interesting in some contexts, such as the codes given in Table 2, where it is the best known bound (as mentioned in Remarks 4 and 5, we recall that other state-of-the-art bounds do not apply).*

Remark 7. *In some very particular cases (when their length is comparable with competing codes), expanded LCD Reed-Solomon codes (covered in Sec. 3.2) can be interesting substitutes to LCD generalized residue codes. For exemple, there is in Table 2 a binary code of dimension* 6440*, length* $113^2 = 12769$*, and minimal distance* ≥ 11*. The expanded LCD Reed-Solomon code of Example 2 has the same dimension, but a smaller length (only* 10230*) and a minimal distance equal or greater than* 380*.*

4. Constructing LCD codes from other codes.

The constructions investigated in the previous section do not always allow to reach the precise parameters (length, dimension, minimum distance) needed in our framework. We must then study those secondary constructions which allow modifying the parameters of codes and to obtain LCD codes from other codes (which can be LCD or not). As far as we know, these secondary constructions have not yet been studied in the literature.
The LCD property is invariant under permutation of the codeword coordinates and, as seen in Subsection 3.2, under expansion. The only two other transformations that we know which preserve the LCD property are the direct sum and the direct product. They are detailed in Sec. 4.1. These preservations do not allow to construct LCD codes with large rate. But transformations of codes which do not preserve the LCD property can allow more constructions of LCD codes. Let ϕ be one of them. Then, we can express by means of a code C the fact that $\phi(C)$ is LCD, or by means of $\phi(C)$ the fact that C is LCD. This allows to have constraints different from $C \cap C^\perp = \{0\}$, that could possibly be satisfied by other classes of codes. The operations allowing to turn codes into LCD are studied in Sec. 4.2, which discusses puncturing, shortening, extending and the $(u, u+v)$ construct. These operations allow to fine-tune a code, with a view to obtain LCD codes with adjusted parameters. Finally, Sec. 4.3 explains how to turn an arbitrary code into a LCD code by applying a linear automorphism.

4.1. Transformations of LCD codes into other LCD codes.

4.1.1. *Constructing LCD codes using the direct sum.*

Proposition 10. *If C_1 and C_2 are LCD codes of respective parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, then their* direct sum *(i.e. their Cartesian product), defined as $C_1 \oplus C_2 = \{(c_1, c_2), c_1 \in C_1, c_2 \in C_2\}$, is LCD of parameters $[n_1+n_2, k_1+k_2, \min(d_1, d_2)]$.*

The name of *direct sum* (see [19, Problem 17 of Chp. 1, page 76]) comes from the fact that the indices of the codewords of C_1 and of those of C_2 being distinct, the sum of $C_1 \times \{0\}$ and $\{0\} \times C_2$ as vector-spaces is direct.

Proof. $(C_1 \oplus C_2)^\perp = C_1^\perp \oplus C_2^\perp$ and then $(C_1 \oplus C_2) \cap (C_1 \oplus C_2)^\perp = (C_1 \cap C_1^\perp) \oplus (C_2 \cap C_2^\perp)$. □

4.1.2. *Constructing LCD codes using the direct product.*

Definition 4.1 (Direct Product, [19, Chap. 18, §2, page 568])**.** Let C_1 and C_2 be two codes of parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$, respectively. The direct product $C_1 \otimes C_2$ between C_1 and C_2 is the code of parameters $[n_1 n_2, k_1 k_2, d_1 d_2]$, whose codewords are equal to:

$$(c_1[j_1]c_2[j_2])_{0 \le j_1 < n_1, 0 \le j_2 < n_2}, \tag{4}$$

for all $c_1 \in C_1$ and $c_2 \in C_2$, where the square brackets operator represents the coordinate selection of a codeword.

Remark 8. *The codewords of $C_1 \otimes C_2$ can have their coordinates permuted such that they write:*

- *either as $(c_1[j_1]c_2)_{0 \le j_1 < n_1}$,*
- *or as $(c_2[j_2]c_1)_{0 \le j_2 < n_2}$,*

where words such as $c_1[j_1]c_2$, where $c_1[j_1] \in \mathbb{F}_q$ and $c_2 \in \mathbb{F}_q^{n_2}$, belong to $\mathbb{F}_q^{n_2}$.

Definition 4.2. We denote:

- by $\sigma_1 : \{0, \ldots, n_1 \times n_2 - 1\} \to \{0, \ldots, n_1 \times n_2 - 1\}$ the permutation of coordinates that leads to codewords of $C_1 \otimes C_2$ been written as $(c_1[j_1]c_2)_{0 \le j_1 < n_1}$,
- by $\sigma_2 : \{0, \ldots, n_1 \times n_2 - 1\} \to \{0, \ldots, n_1 \times n_2 - 1\}$ the permutation of coordinates that leads to codewords of $C_1 \otimes C_2$ been written as $(c_2[j_2]c_1)_{0 \le j_2 < n_2}$.

More precisely, let $d = (c_1[j_1]c_2[j_2])_{0 \le j_1 < n_1, 0 \le j_2 < n_2}$ a codeword of $C_1 \otimes C_2$ (see Eqn. (4)). We denote: $d[j] = c_1[j/n_2]c_2[j \mod n_2]$, for all $0 \le j < n_1 n_2$. Then:

$$\begin{cases} \sigma_1(j) & = j \ , \\ \sigma_2(j) & = n_2(j \mod n_1) + (j/n_1) \ . \end{cases}$$

Lemma 4.3. *The dual of $C_1 \otimes C_2$ is $(C_1^\perp \otimes \mathbb{F}_q^{n_2}) + (\mathbb{F}_q^{n_1} \otimes C_2^\perp)$.*

Proof. In fact it is easily shown that the dual of $C_1 \otimes C_2$ also equals $(C_1^\perp \otimes C_2) + (\mathbb{F}_q^{n_1} \otimes C_2^\perp)$ (this is between the lines of the proof of Proposition 11 below) when C_1 and C_2 are LCD. Actually, the sum in Lemma 4.3 is not direct, but the sum $(C_1^\perp \otimes C_2) + (\mathbb{F}_q^{n_1} \otimes C_2^\perp)$ or $(\mathbb{F}_q^{n_1} \otimes C_2) + (C_1 \otimes C_2^\perp)$ (both equal to the dual of $C_1 \otimes C_2$) is indeed direct. □

Proposition 11. *If C_1 and C_2 are LCD, then $C_1 \otimes C_2$ is also LCD.*

Proof. We know that a linear code C of length n is LCD if and only if $C + C^\perp = \mathbb{F}_q^n$, since the dimension of $C^\perp$ equals the co-dimension of C. The code $(C_1 \otimes C_2) + (C_1^\perp \otimes \mathbb{F}_q^{n_2})$ includes $(C_1 + C_1^\perp) \otimes C_2 = \mathbb{F}_q^{n_1} \otimes C_2$, since any word $((c_1[j_1] + c_1'[j_1])c_2)_{0 \le j_1 < n_1}$ of $(C_1 + C_1^\perp) \otimes C_2$ can be decomposed into the sum of $(c_1[j_1]c_2)_{0 \le j_1 < n_1} \in C_1 \otimes C_2$ and of $(c_1'[j_1]c_2)_{0 \le j_1 < n_1} \in C_1^\perp \otimes C_2 \subseteq C_1^\perp \otimes \mathbb{F}_q^{n_2}$. Hence $(C_1 \otimes C_2) + (C_1^\perp \otimes \mathbb{F}_q^{n_2}) + (\mathbb{F}_q^{n_1} \otimes C_2^\perp)$ includes $\mathbb{F}_q^{n_1} \otimes C_2 + \mathbb{F}_q^{n_1} \otimes C_2^\perp = \mathbb{F}_q^{n_1} \otimes \mathbb{F}_q^{n_2} = \mathbb{F}_q^{n_1 n_2}$. □

Proposition 12. *Let C_1 and C_2 be two linear codes of dual distance $d_1^\perp$ and $d_2^\perp$. Then, the dual distance of $C_1 \otimes C_2$ is $\min(d_1^\perp, d_2^\perp)$.*

Example 3. Let $q = 2$, $n = 15$ and $k = 8$. The best known linear code in the Magma database has parameters $[15, 8, 4]$. But this code is not LCD. However, let C_1 the cyclic linear code of parameters $[5, 4, 2]$ of generating matrix $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$, and C_2 the cyclic linear code of parameters $[3, 2, 2]$ of generating matrix $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. As C_1 and C_2 are LCD, then, by Proposition 11, $C_1 \otimes C_2$ is also LCD, and has parameters $[5 \times 3, 4 \times 2, 2 \times 2] = [15, 8, 4]$.

4.1.3. *The $(u, u + v)$ construction.* The $(u, u + v)$ construction (also known as the Plotkin sum) provides an interesting construction of LCD codes.

Proposition 13. *If C and C' are linear codes of parameters $[n, k, d]$ and $[n, k', d']$, respectively, and if $C' \cap C^\perp$ is LCD (that is, $C + C'^\perp$ is LCD) and $C \cap C'^\perp = \{0\}$, then the code $C'' = \{(u, u + v),\ u \in C, v \in C'\}$ is LCD of parameters $[2n, k + k', \min(2d, d')]$.*

Proof. We have $C''^\perp = \{(a, b),\ a + b \in C^\perp, b \in C'^\perp\}$ and then $C'' \cap C''^\perp = \{(a, b),\ a + b \in C' \cap C^\perp, a \in C, b \in C'^\perp\}$. For any such (a, b), the double condition $a \in C, b \in C'^\perp$ implies $a + b \in C + C'^\perp$. Hence, $a + b \in (C + C'^\perp) \cap (C + C'^\perp)^\perp$ and $a = b$ since $C + C'^\perp$ is assumed LCD. Then $a = b \in C \cap C'^\perp$ is null. □

Note that the double condition "$C' \cap C^\perp$ is LCD and $C \cap C'^\perp = \{0\}$" is satisfied when C and $C'^\perp$ are supplementary in $\mathbb{F}_q^n$ since we have then $C' \cap C^\perp = C \cap C'^\perp = \{0\}$, but this double condition is much more general. In fact, the building blocks for this construction are a LCD code $\mathcal{C}$, two subcodes C_1 and C_2 of $\mathcal{C}$ which are supplementary in $\mathcal{C}$; we take then $C = C_1$ and $C' = C_2^\perp$. Note that the rate of $\mathcal{C}$ is $\frac{k+n-k'}{2n}$, the rate of its dual is $\frac{k'+n-k}{2n}$, while that of the $(u, u+v)$-constructed code is $\frac{k+k'}{2n}$. Hence, this construction allows increasing the rate in some cases.

4.2. **Constructing LCD codes by puncturing, shortening and extending codes.**

4.2.1. *Puncturing and shortening codes.* Let C be a binary linear code of length n and let $T \subseteq \{1, \ldots, n\}$. Let C^T be the *punctured* code obtained by deleting every coordinate c_i such that $i \in T$ in every codeword c of C and C_T be the *shortened* code obtained by deleting every such coordinate in every codeword c of C such that $c_i = 0$ for every $i \in T$. Then (see [16, Chap. 1, Theorem 1.5.7, page 17]):

$$(C^T)^\perp = (C^\perp)_T.$$

This can be easily checked: $(C^\perp)_T \subseteq (C^T)^\perp$ is clear and every element of $(C^T)^\perp$ can be extended to an element of $C^\perp$ by adding zeroes, which proves that $(C^T)^\perp \subseteq (C^\perp)_T$. By applying this property to $C^\perp$, we have also:

$${C_T}^\perp = (C^\perp)^T.$$

Puncturing and shortening allow constructing LCD codes but the conditions on the original code C and on its dual are not straightforward to check.

Proposition 14. *Let C be a linear $[n, k, d]$ code and T a subset of $\{1, \ldots, n\}$. Then:*

1. *The shortened code C_T is LCD if and only if every $c \in C$, whose support is disjoint from T and for which there exists $c' \in C^\perp$ coinciding with c outside T, is null. Code C_T has parameters $[n-|T|, k', d']$ with $k-|T| \leq k' \leq k$ and $d' \geq d$.*
2. *The punctured code C^T is LCD if and only if $(C^\perp)_T$ is LCD, that is, every $c' \in C^\perp$, whose support is disjoint from T and such that there exists $c \in C$ coinciding with c' outside T, is null. Code C^T has parameters $[n-|T|, k, d']$, with $d' \geq d-|T|$ if $d > |T|$.*

Proof. We have ${C_T}^\perp = (C^\perp)^T$ and $C_T \cap (C^\perp)^T$ contains a nonzero vector if and only if there exists $c \in C$ nonzero whose support is disjoint from T and $c' \in C^\perp$ which coincides with c outside T. This proves 1 (the parameters of C_T and C^T are well known, see e.g. [16, Chap. 1.5]).
The fact that C^T is LCD if and only if $(C^\perp)_T$ is LCD is a direct consequence of ${C_T}^\perp = (C^\perp)^T$. Applying the characterization of the LCD property of C_T to $C^\perp$ gives 2. □

We investigate now hypotheses under which the conditions of Proposition 14 are satisfied.

Corollary 1. *Let C be a linear code of length n and let T be a subset of $\{1, \ldots, n\}$ whose size is strictly smaller than the minimum distance of $C + C^\perp$ and such that every nonzero codeword of $C \cap C^\perp$ has a nonzero coordinate at one (at least) of the positions in T. Then C_T and C^T are LCD codes.*

Proof. Indeed, the vector $c + c'$ in 1 or 2 of Proposition 14 has support included in T and has then Hamming weight strictly smaller than the minimum distance of $C + C^\perp$ and is then null. Hence $c = c'$ has all its coordinates at positions in T null, and is then null, according to the hypothesis on T. □

Corollary 2. *Let C be a LCD code of length n and let T be a subset of $\{1, \ldots, n\}$ whose size is strictly smaller than the dual distance of C (the minimum distance of $C^\perp$). Let π be the linear projection over C parallel to $C^\perp$ (for every $x \in \mathbb{F}_q^n$, $\pi(x)$ is the unique element of C such that $x \in \pi(x) + C^\perp$). Let E_T be the vector space $\{x \in \mathbb{F}_q^n\,;\, supp(x) \subseteq T\}$ where $supp(x)$ is the support $\{i\,;\, x_i \neq 0\}$ of x, and let π_T be the linear function from E_T to $\mathbb{F}_q^T$ such that $\pi_T(x)$ is the restriction of the vector $\pi(x)$ to the positions in T. Then C_T is LCD if and only if π_T is bijective.*

Proof. We first show that the condition of bijectivity of π_T is sufficient. Let $c \in C$ be nonzero and have support disjoint from T, and let $c' \in C^\perp$ be such that c and c' coincide outside T. Let $x = c + c'$. Then x belongs to E_T and is nonzero since C and $C^\perp$ are supplementary. Then $\pi_T(x)$ is nonzero, that is, $supp(\pi(x)) \cap T \neq \emptyset$, but by definition $\pi(x) = c$, a contradiction. We deduce according to Proposition 14 that C is LCD.
Let us prove now that the condition is necessary. Let $x \in E_T$ be nonzero and let $c \in C$ and $c' \in C^\perp$ be the unique elements such that $x = c + c'$. Then c is nonzero since if $c = 0$ then $x \in C^\perp$, a contradiction since x has Hamming weight strictly smaller than the minimum distance of $C^\perp$. Moreover, c and c' coincide outside T. Then, according to Proposition 14, c has nonzero coordinates among the positions in T and $\pi_T(x) \neq 0$. Hence π_T is injective and therefore bijective since the vector spaces E_T and $\mathbb{F}_q^T$ have the same dimension $|T|$. □

The next corollary deals with cyclic codes. We index then the coordinates of the codewords by $0, \ldots, n-1$ instead of $1, \ldots, n$.

Corollary 3. *Let C be a LCD cyclic code of length n over $\mathbb{F}_q$. Let $E(X)$ be the idempotent of C. Let $T = \{n-t, n-t+1, \ldots, n-1\}$ where $1 \leq t \leq n-1$. Then the shortened code C_T is LCD if and only if, for every nonzero polynomial $f(X) = f_{n-t}X^{n-t} + \cdots + f_{n-1}X^{n-1} \in \mathbb{F}_q[X]$, the polynomial $f(X)E(X)$ [mod $X^n - 1$] has degree at least $n-t$. In particular, if $t = 1$ then C_T is LCD if and only if the constant coefficient of $E(X)$ is nonzero (i.e. equals 1 if $q = 2$).*

Proof. Given a vector $(g_0, \ldots, g_{n-1})$ represented by the polynomial $g(X) = g_0 + g_1X + \cdots + g_{n-1}X^{n-1}$, the projection of $g(X)$ on C parallel to $C^\perp$ is represented by the product $g(X)E(X)$ computed in $\mathbb{F}_q[X]/(X^n - 1)$ (indeed, the idempotent of $C^\perp$ is $E(X) + 1$ and we have $g(X) = g(X)E(X) + g(X)(E(X) + 1)$). According to Corollary 2, C_T is then LCD if and only if, for every nonzero polynomial $f(X) = f_{n-t}X^{n-t} + \cdots + f_{n-1}X^{n-1}$, the polynomial $f(X)E(X)$ [mod $X^n - 1$] has degree at least $n - t$. If $t = 1$ this condition is equivalent to the fact that the constant coefficient of $E(X)$ is nonzero. □

Example 4. Let C be the binary QR code of length $n = 89$; this cyclic code is LCD because $n \mod 8 = +1$. It can be checked with Magma that the code C_T is LCD for $T = \{n-1\}, \{n-2, n-1\}, \{n-3, n-2, n-1\}$. A computer search allows to check Corollary 3 for those values of T. However, $C_{\{n-4,n-3,n-2,n-1\}}$ is not LCD. This complies with Corollary 3, since, for instance, for $f(X) = X^{85} + X^{88}$ (i.e., $f_{n-4} = 1$, $f_{n-3} = 0$, $f_{n-2} = 0$, $f_{n-1} = 1$), we have $f(X)E(X) = X^3 + X^5 + X^6 + X^8 + X^9 + X^{10} + X^{12} + X^{13} + X^{14} + X^{15} + X^{18} + X^{19} + X^{20} + X^{24} + X^{28} + X^{30} + X^{31} + X^{32} + X^{33} + X^{36} + X^{39} + X^{40} + X^{44} + X^{45} + X^{48} + X^{51} + X^{52} + X^{53} + X^{54} + X^{56} + X^{60} + X^{64} + X^{65} + X^{66} + X^{69} + X^{70} + X^{71} + X^{72} + X^{74} + X^{75} + X^{76} + X^{78} + X^{79} + X^{81}$, which has degree $81 < n - 4$.

In the framework of Corollary 3, let $E(X) = \sum_{j=0}^{n-1} e_j X^j$, then C_T is LCD if and only if the polynomials $\sum_{j=n-t-i}^{n-1-i} e_j X^{i+j}$, where i ranges from $n-t$ to $n-1$, are linearly independent. Note that the matrix G whose i-th row is the list of the coefficients of the polynomial $X^i E(X)$ [mod $X^n - 1$], where i ranges over an interval of length k (the dimension of C), say where $i \in \{n-k, \ldots, n-1\}$, is a generator matrix of C. According to Corollary 3, C_T is LCD if and only if the submatrix of the last t rows and the last t columns of G is non-degenerate, that is, the set $\{n-t, \ldots, n-1\}$ is an information set of the subcode of C generated by the last t rows of G.

Example 5. Let C be the QR (cyclic) binary $[17, 9, 5]$-code whose zeroes are β^i, $i = 1, 2, 4, 8, 9, 13, 15, 16$ where β is a primitive n-th root of unity. The generator polynomial of C is $X^8 + X^7 + X^6 + X^4 + X^2 + X + 1$. The shortened $C_{\{17\}}$ code is LCD, of parameters $[16, 8, 5]$. This code is indicated as having optimal parameters in the Grassl table [14] and is an example of LCD code given in [8, Appendix B]. Notice that this $[16, 8, 5]$ code is equivalent to the code of Example 1 punctured at $\{17\}$.

We obtain similar corollaries for characterizing the fact that C^T is LCD when C is LCD, by exchanging the roles of C and $C^\perp$.

4.2.2. *Extending codes.* Let C be a binary linear code of length n. Let us extend it by adding a coordinate $\ell(x)$ to each codeword $x \in C$, where ℓ is a linear form on C. We assume that there exists $a \in C$ such that $\ell(a) = 1$ so that this extension of the code is not just adding a zero.

Proposition 15. *Let C be a linear code and $\widehat{C} = \{(x, \ell(x)),\ x \in C\}$, where ℓ is a nonzero linear form on C. Let $a \in C$ be such that $\ell(a) = 1$ and let us denote $\langle a, x\rangle$ by $\ell'(x)$. Then $\widehat{C}$ is LCD if and only if :*

$$C \cap (\ker(\ell))^\perp \cap \ker(\ell + \ell') = \{0\}.$$

Proof. According to the hypothesis, $\ker(\ell)$ is a hyperplane of C, and C is the direct sum of $\ker(\ell)$ and $\{0, a\}$. Denoting by $\langle , \rangle$ the usual inner product in $\mathbb{F}_q^n$, we have then:

$$\begin{aligned}(\widehat{C})^\perp &= \{(x, \epsilon) \in \mathbb{F}_q^n \times \mathbb{F}_q\,;\, \forall c \in C,\ \langle c, x\rangle = \epsilon\, \ell(c)\}\\ &= \big\{(x, \epsilon) \in \mathbb{F}_q^n \times \mathbb{F}_q\,;\, \forall c \in \ker(\ell),\ \langle c, x\rangle = 0 \text{ and } \langle a, x\rangle = \epsilon\big\}\\ &= \{(x, \langle a, x\rangle);\ x \in (\ker(\ell))^\perp\}.\end{aligned}$$

Hence $\widehat{C} \cap (\widehat{C})^\perp = \{(x, \langle a, x\rangle);\ x \in C \cap (\ker(\ell))^\perp \text{ and } \langle a, x\rangle = \ell(x)\}$. □

Note that if C has dimension k then $(C \cap \ker(\ell))^\perp$ has dimension $n - k + 1$ and $C \cap (C \cap \ker(\ell))^\perp$ has then dimension at least 1.

The particular case where this dimension equals 1 is of course particularly interesting. Note that $(C \cap \ker(\ell))^\perp$ is the union of $C^\perp$ and of one of its cosets, then if C is LCD, $C \cap (C \cap \ker(\ell))^\perp$ has dimension 1.

The condition becomes then that the unique nonzero element of $C \cap (C \cap \ker(\ell))^\perp$ does not belong to $\ker(\ell + \ell')$.

Example 6. Let C as in Example 5. The generator matrix G of C is:

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

that can be extended thanks to $\ell : x \in \mathbb{F}_2^{17} \mapsto x(1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)^\mathsf{T}$, giving

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

This matrix generates a LCD code of parameters $[18, 9, 5]$.

The vector a can be chosen as the first line of G, that is:

$$a = (1,0,0,0,0,0,0,0,0,1,0,0,1,1,1,0,0) \ ,$$

thus the form ℓ' is defined as $\ell'(x) = \langle a, x\rangle$. The code $C \cap (C \cap \ker(\ell))^{\perp}$ is generated by $M_1 = (1,1,0,1,1,1,0,0,1,0,1,0,0,1,1,1,0)$, $\ker(\ell + \ell')$ is generated by $M_2 = (0,1,0,0,0,0,0,0,0,1,0,0,1,1,1,0,0)^{\mathsf{T}}$, and indeed, $M_1 M_2 = (1)$.

We notice that the best linear code of length 18 and dimension 9 has parameters $[18, 9, 6]$. However, the code example given by Magma is not LCD.

4.3. **LCD codes obtained by applying a linear automorphism to a given code.** Let C be a linear code of length n and L a linear automorphism of $\mathbb{F}_q^n$. We consider the code $L(C) = \{L(c),\, c \in C\}$. Note that every linear code of length n and dimension k can be obtained from one such code by applying all linear automorphisms. We denote by L^* the adjoint operator of L, characterized by the fact that, for every $x, y \in \mathbb{F}_q^n$, we have $\langle x, L(y)\rangle = \langle L^*(x), y\rangle$, and whose matrix is the transpose of that of L.

Proposition 16. *Let C be any linear code of length n and dimension k. Let $\mathcal{L}$ be the space of linear automorphisms of $\mathbb{F}_q^n$. The set of LCD codes of length n and dimension k equals $\{L(C);\, L \in \mathcal{L},\, C^{\perp} \cap (L^* \circ L(C)) = \{0\}\}$.*

Proof. The dual of $L(C)$ equals ${L^*}^{-1}(C^{\perp})$ since for every $x \in \mathbb{F}_q^n$ and every $c \in C$, we have that $\langle L(c), x\rangle = 0$ for every $c \in C$ if and only if $L^*(x) \in C^{\perp}$. Given C of dimension k, finding all LCD codes of length n and dimension k is then equivalent to finding all linear automorphisms L such that : $C^{\perp} \cap (L^* \circ L(C)) = \{0\}$. □

The applications $L^* \circ L$ are all the self-adjoint automorphisms A (whose matrices are invertible and symmetric). Using this proposition for constructing a LCD code corresponds to (1) determining an auto-adjoint automorphism $A \in \mathcal{L}$ such that $C^{\perp} \cap A(C) = \{0\}$ and (2) finding $L \in \mathcal{L}$ such that $A = L^* \circ L$.

Example 7. The best known linear code of length 7 and dimension 4 over $\mathbb{F}_2$ has minimum distance 3. However, we have checked by computer search that no LCD code of parameters $[7, 4, 3]$ exists. LCD codes of parameters $[7, 4, 2]$ exist, and can be obtained by Proposition 16, starting from the Hamming code for C.

If C is already LCD, for instance $C = \mathbb{F}_q^k \times \{0\}$, denoting by A_i the i-th coordinate function of A, the condition $C^{\perp} \cap (A(C)) = \{0\}$ is that $(A(x) \in C^{\perp}$ and $x \in C)$ implies $x = 0$, that is, $A_1(x) = \cdots = A_k(x) = x_{k+1} = \cdots = x_n = 0$ implies $x = 0$, that is the mapping $x \mapsto (A_1(x), ..., A_k(x), x_{k+1}, ..., x_n)$ is bijective, that is, the mapping $x \mapsto ({L^*}_1(x), ..., {L^*}_k(x), L_{k+1}^{-1}(x), ..., L_n^{-1}(x))$ is bijective.

5. **Conclusion and perspectives.** Complementary dual codes have applications in information protection. An example is that of a cryptographic implementation, be it hardware or software, which must be simultaneously protected against information leakage and information corruption, since both threats enable successful attacks. We construct cyclic LCD codes, which can be used for that and need then to have large minimum distance and large rate, and find suitable codes within Reed-Solomon codes and the class of generalized residue codes. In addition to these codes, we detail some secondary constructions, using direct sum, direct product, puncturing, shortening, extension, $(u, u + v)$ construction, and the application of a suitable linear automorphism.

As a perspective, we aim at defining bounds for the minimum distance of LCD codes, and at finding codes that approach those bounds. Besides, LCD codes of *sparse* generator matrices would help reduce the implementation complexity.

Acknowledgments. The authors are grateful to Patrick Solé for pointing relevant previous art. We also thank Mehdi Tibouchi for raising our attention on the original properties of the $[16, 8, 5]$ linear code.

References

[1] Stephen Barnett. *Matrices: Methods and Applications*. Applied Mathematics & Computing Science Series. Oxford Applied Mathematics & Computing Science Series, June 21 1990.

[2] Koichi Betsumiya and Masaaki Harada. Binary optimal odd formally self-dual codes. *Des. Codes Cryptography*, 23(1):11–22, 2001. On-line version: http://www.math.nagoya-u.ac.jp/~koichi/paper/fsd-odd.pdf [accessed on August 4, 2015].

[3] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. A Low-Entropy First-Degree Secure Provable Masking Scheme for Resource-Constrained Devices. In *Proceedings of the Workshop on Embedded Systems Security*, WESS '13, pages 7:1–7:10, New York, NY, USA, September 29 2013. ACM. Montreal, Quebec, Canada. DOI: 10.1145/2527317.2527324.

[4] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm, and Xuan Thuy Ngo. Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses. In *2015 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2015, pages 82–87, McLean, VA, USA*, May 5-7 2015. DOI: 10.1109/HST.2015.7140242.

[5] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Thuy Ngo, and Laurent Sauvage. Hardware Trojan Horses in Cryptographic IP Cores. In *FDTC*, pages 15–29, August 20 2013. Santa Barbara, CA, USA.

[6] Shivam Bhasin, and Jean-Luc Danger Xuan Thuy Ngo, Sylvain Guilley, and Zakaria Najm. Encoding the State of Integrated Circuits: A Proactive and Reactive Protection against Hardware Trojans Horses. In *Proceedings of the 9th Workshop on Embedded Systems Security*, WESS '14, New York, NY, USA, October 17 2014. ACM. New Dehli, India. DOI: 10.1145/2668322.2668329.

[7] A. Bojilov, A.J. van Zanten, and S.M. Dodunekov. Minimal Distances in Generalized Residue Codes. *Proceedings of Twelfth International Workshop of Algebraic and Combinatorial Coding Theory* ACCT-2010, Novosibirsk, Russia, September 2010, ISBN: 9785861341745. Book edited by the Sobolev Institut of Mathematics. 334 pages.

[8] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssem Maghrebi. Orthogonal Direct Sum Masking – A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks. In *WISTP*, volume 8501 of *LNCS*, pages 40–56. Springer, June 2014. Heraklion, Greece.

[9] Claude Carlet. Boolean Functions for Cryptography and Error Correcting Codes: Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering. pages 257–397. Cambridge University Press, Y. Crama and P. Hammer eds, 2010. Preliminary version available at: http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf.

[10] Claude Carlet, Abderrahman Daif, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm, Xuan Thuy Ngo and Cédric Tavernier. Optimized Linear Complementary Codes Implementation for Hardware Trojan Prevention. In *22nd European Conference on Circuit Theory and Design, ECCTD2015*, August 24-26 2015, Trondheim, Norway.

[11] Claude Carlet, Philippe Gaborit, Jon-Lark Kim, and Patrick Solé. A New Class of Codes for Boolean Masking of Cryptographic Computations. *IEEE Transactions on Information Theory*, 58(9):6000–6011, 2012.

[12] Bocong Chen, Hai Q. Dinh, and Hongwei Liu. Repeated-root constacyclic codes of length $2\ell^m p^n$. *CoRR*, abs/1406.1848, 2014.

[13] Jalal Etesami, Fangning Hu, and Werner Henkel. LCD Codes and Iterative Decoding by Projections, a First Step Towards an Intuitive Description of Iterative Decoding. In *GLOBECOM*, pages 1–4. IEEE, 2011.

[14] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de/, 2007. Accessed on 2012-07-23.
[15] Vincent Grosso, François-Xavier Standaert, and Emmanuel Prouff. Low Entropy Masking Schemes, Revisited. In Aurélien Francillon and Pankaj Rohatgi, editors, *CARDIS*, volume 8419 of *LNCS*, pages 33–43. Springer, 2013.
[16] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Jun 26 2003.
[17] W. B. Vasantha Kandasamy Kandasamy, Florentin Smarandache, R. Sujatha, and R. S. Raja Durai. *Erasure Techniques in MRD codes*. April 28 2012. ISBN-10: 1599731770, ISBN-13: 978-1599731773.
[18] San Ling and Chaoping Xing. Polyadic codes revisited. *IEEE Transactions on Information Theory*, 50(1):200–207, 2004.
[19] F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, North Holland, 1977. ISBN: 978-0-444-85193-2.
[20] James L. Massey. Linear codes with complementary duals. *Discrete Mathematics*, 106-107:337–342, 1992.
[21] Gary L. Mullen and Daniel Panario. *Handbook of Finite Fields*. Chapman and Hall/CRC, June 17 2013. ISBN 9781439873786 - CAT# K13417.
[22] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Trans. Computers*, 58(6):799–811, 2009.
[23] Nicolas Sendrier. Linear Codes with Complementary Duals Meet the Gilbert-Varshamov Bound. *Discrete Mathematics*, 285:345–347, 2004.
[24] Anuradha Sharma, Gurmeet K. Bakshi, and Madhu Raka. Polyadic codes of prime power length. *Finite Fields and Their Applications*, 13(4):1071–1085, 2007.
[25] Jacobus H. van Lint and F. Jessie MacWilliams. Generalized quadratic residue codes. *IEEE Transactions on Information Theory*, 24(6):730–737, 1978.
[26] Harold N. Ward. Quadratic Residue Codes and Divisibility. In *Handbook of Coding Theory, V.S. Pless & W.C. Huffman (Editors), Elsevier Science*, pages 827–870, 1998.
[27] Xiang Yang and James L Massey. The condition for a cyclic code to have a complementary dual. *Discrete Mathematics*, 126(1):391–393, 1994.

Appendix: Tables. In both tables 1 and 2, the binary linear codes are quadratic residues ($t = 2$), and have parameters $[n, k, d]$, where $k = n - \mathsf{card}(Q)$ and the minimum distance d is greater or equal to the BCH bound.

The cells in gray in Table 1 correspond to composite length, i.e., the length n is not a prime power, as opposed to the cells in white. The cells in gray correspond to codes of rate near $1/4$. They all correspond to duals of QR codes direct products (recall Sec. 4.1.2). For instance, the code of length $n = 697$ and dimension $k = 697 - 189$ is the dual of the direct product of QR codes C_1 and C_2 of parameters $[17, 9]$ and $[41, 21]$ (notice that $697 = 17 \times 41$ and $189 = 9 \times 21$). Therefore, the minimum distance of this code is small, namely 6. Indeed, we can apply Proposition 12, where the dual distance $d_1^\perp$ of C_1 is equal to 6, and the dual distance $d_2^\perp$ of C_2 is equal to 10.

In Tab. 2, the minimum distance are given as:

1. the BCH lower bound,
2. the QR lower bound (see Proposition 9),
3. the (exact) value calculated by Magma; we fix a timeout of 1 hour.

The cells in gray highlight the best value or bound for the minimum distance. Starting from $p \geq 113$, it seems that the bound of Proposition 9 (i.e., $d \geq \lceil \sqrt{p} \rceil$) is the most efficient.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: claude.carlet@univ-paris8.fr
E-mail address: sylvain.guilley@telecom-paristech.fr

TABLE 1. Values of $n \in \mathbb{N}$ (with its factorization) such that $2, -1 \in Q$, for $t = 2$, and Q has size strictly smaller than $\frac{n+1}{2}$

n		$\mathsf{card}(Q)$	BCH bound
289	$= 17^2$	137	6
697	$= 17 \times 41$	189	6
1241	$= 17 \times 73$	333	6
1513	$= 17 \times 89$	405	6
1649	$= 17 \times 97$	441	6
1681	$= 41^2$	821	6
1921	$= 17 \times 113$	513	6
2329	$= 17 \times 137$	621	6
2993	$= 41 \times 73$	777	6
3281	$= 17 \times 193$	873	6
3649	$= 41 \times 89$	945	6
3961	$= 17 \times 233$	1053	6
3977	$= 41 \times 97$	1029	6
4097	$= 17 \times 241$	1089	6
4369	$= 17 \times 257$	1161	6
4633	$= 41 \times 113$	1197	6
4777	$= 17 \times 281$	1269	6
4913	$= 17^3$	2321	6
5321	$= 17 \times 313$	1413	6
5329	$= 73^2$	2629	10
5617	$= 41 \times 137$	1449	6
5729	$= 17 \times 337$	1521	6
6001	$= 17 \times 353$	1593	6
6497	$= 73 \times 89$	1665	6
6817	$= 17 \times 401$	1809	6
6953	$= 17 \times 409$	1845	6
7081	$= 73 \times 97$	1813	10
7361	$= 17 \times 433$	1953	6
7633	$= 17 \times 449$	2025	6
7769	$= 17 \times 457$	2061	6
7913	$= 41 \times 193$	2037	6
7921	$= 89^2$	3917	6
8249	$= 73 \times 113$	2109	6
8633	$= 89 \times 97$	2205	6
8857	$= 17 \times 521$	2349	6
9409	$= 97^2$	4657	10
9553	$= 41 \times 233$	2457	6
9673	$= 17 \times 569$	2565	6
9809	$= 17 \times 577$	2601	6
9881	$= 41 \times 241$	2541	6

TABLE 2. Values of p (prime number) and $n = p^2$ such that $2, -1 \in Q$, for $t = 2$, the size of Q and BCH bound

p	n	$\mathsf{card}(Q)$	Minimum distance d		
			d_{BCH}	$\lceil\sqrt{p}\rceil$	d_{Magma}
17	289	137	≥ 6	≥ 5	$= 6$
41	1681	821	≥ 6	≥ 7	$= 9$
73	5329	2629	≥ 10	≥ 9	?
89	7921	3917	≥ 6	≥ 10	?
97	9409	4657	≥ 10	≥ 10	?
113	12769	6329	≥ 6	≥ 11	?
137	18769	9317	≥ 7	≥ 12	?
193	37249	18529	≥ 10	≥ 14	?
233	54289	27029	≥ 7	≥ 16	?
241	58081	28921	≥ 14	≥ 16	?
257	66049	32897	≥ 7	≥ 17	?
281	78961	39341	≥ 7	≥ 17	?