Designs, Codes and Cryptography, 6, 21–35 (1995)

Modular and p-adic Cyclic Codes

A. R. CALDERBANK AND N. J. A. SLOANE
Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974

Received August 4, 1994

Abstract. This paper presents some basic theorems giving the structure of cyclic codes of length n over the ring of integers modulo p^a and over the p-adic numbers, where p is a prime not dividing n. An especially interesting example is the 2-adic cyclic code of length 7 with generator polynomial $X^3 + \lambda X^2 + (\lambda - 1)X - 1$, where λ satisfies $\lambda^2 - \lambda + 2 = 0$. This is the 2-adic generalization of both the binary Hamming code and the quaternary octacode (the latter being equivalent to the Nordstrom-Robinson code). Other examples include the 2-adic Golay code of length 24 and the 3-adic Golay code of length 12.

1. Introduction

This paper was prompted by the following questions. It is known [14], [16] that the binary polynomial $X^3 + X + 1$ that generates the cyclic Hamming code of length 7 lifts to a polynomial $X^3 + 2X^2 + X + 3$ over $\mathbb{Z}_4$ that generates the octacode, equivalent to the binary nonlinear Nordstrom-Robinson code. What codes are obtained if we continue to lift this polynomial to $\mathbb{Z}_8$, $\mathbb{Z}_{16}$, ..., and even to the 2-adic integers $\mathbb{Z}_{2^\infty}$? What is the general structure of cyclic codes over these rings? (Solé [23] had already suggested in 1988 that p-adic cyclic codes should be investigated.)

The answer to the first question is given in Example 1 of Section 4, where we describe the "2-adic Hamming code" of length 7 in detail. This is in a certain sense the first interesting 2-adic code. In Examples 2 and 4 we give 2-adic versions of the Golay code and more generally of extended quadratic residue codes of length $8m$, where $8m - 1$ is prime, and a 3-adic version of the Golay code of length 12. Furthermore, this Hamming code and the two Golay codes (and more generally a large class of quadratic residue codes) are all MDS codes. In particular the 2-adic Golay code has minimal Hamming distance 13, even though every projection of it onto the integers modulo 2^a has minimal distance 8. Section 4 also gives p-adic generalizations for other classical families of codes, including BCH, Reed-Muller and quadratic residue codes.

The answer to the second question is given in Theorems 5 and 6 of Section 3, which are the main theoretical results of this paper. It will be seen that modular and p-adic cyclic codes have a simple and elegant structure.

Although cyclic codes over the integers modulo q have been discussed by a number of authors ([5], [6], [9], [12], [21]–[26]), these results seem to have been overlooked.

The results in Section 3, although not at all obvious, are easily verified by the methods of commutative algebra or representation theory [13], [28], so we shall mostly not give proofs.

As far as we know, this paper is the first to consider p-adic codes. (However, several authors ([2], [10], [20]) have studied "global" or complex-valued codes in connection with

the representation theory of $PSL_2(n)$ and other groups, and our p-adic codes are analogues of those complex codes.) For general background on p-adic numbers, see [3], [8], [15], [17].

2. Codes mod p^a and p-adic Codes

We use the symbol $\mathbb{Z}_{p^a}$ to denote the ring $\mathbb{Z}/p^a\mathbb{Z}$ of integers modulo p^a, for any prime p and positive integer a, and $\mathbb{Z}_{p^\infty}$ for the ring of p-adic integers. This slightly unconventional notation has the advantage of allowing us to use $\mathbb{Z}_q$ (where $q = p^a$, $1 \le a \le \infty$) to denote any one of these rings, and allows us to state our results in a uniform way.

An element $u \in \mathbb{Z}_{p^a}$ may be written uniquely as a finite sum

$$u = u_0 + pu_1 + p^2u_2 + \cdots + p^{a-1}u_{a-1},$$

and any element of $\mathbb{Z}_{p^\infty}$ as an infinite sum

$$u = u_0 + pu_1 + p^2u_2 + \cdots,$$

where $0 \le u_i \le p-1$. The units in $\mathbb{Z}_{p^a}$ or $\mathbb{Z}_{p^\infty}$ are precisely the u for which $u_0 \ne 0$. $\mathbb{Z}_{p^a}$ has characteristic p^a, and $\mathbb{Z}_{p^\infty}$ has characteristic 0.

The following definitions and remarks are straightforward generalizations of notions for $\mathbb{Z}_4$ codes given in [12] and [16].

Let $\mathbb{Z}_q = \mathbb{Z}_{p^a}$, where $1 \le a \le \infty$. The set $\mathbb{Z}_q^n$ of n-tuples from $\mathbb{Z}_q$ is of course a $\mathbb{Z}_q$-module, and by a *linear code* over $\mathbb{Z}_q$ we mean any $\mathbb{Z}_q$ sub-module of $\mathbb{Z}_q^n$. We equip $\mathbb{Z}_q^n$ with the inner product $v \cdot w = v_1w_1 + \cdots + v_nw_n$ evaluated in $\mathbb{Z}_q$, and define dual and self-dual codes in the usual way.

A nonzero linear code C over $\mathbb{Z}_{p^a}$, for a finite, has a generator matrix which after a suitable permutation of the coordinates can be written in the form

$$G = \begin{bmatrix} I & A_{01} & A_{02} & A_{03} & \cdots & A_{0,a-1} & A_{0a} \\ 0 & pI & pA_{12} & pA_{13} & \cdots & pA_{1,a-1} & pA_{1a} \\ 0 & 0 & p^2I & p^2A_{23} & \cdots & p^2A_{2,a-1} & p^2A_{2a} \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & p^{a-1}I & p^{a-1}A_{a-1,a} \end{bmatrix}, \tag{1}$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{a-1}, k_a$, and the k_i are nonnegative integers adding to n. This means that C consists of all codewords

$$[v_0 \ v_1 \ v_2 \ \cdots \ v_{a-1}]G,$$

where each v_i is a vector of length k_i with components from $\mathbb{Z}_{p^{a-i}}$, so that C contains p^k codewords, where

$$k = \sum_{i=0}^{a-1}(a-i)k_i.$$

We say that C has *type*[1]

$$1^{k_0} p^{k_1} (p^2)^{k_2} \cdots (p^{a-1})^{k_{a-1}}. \tag{2}$$

The zero code (containing only the zero codeword) has type 1^0. It is easy to see that the code C with generator matrix (1) has a dual $C^\perp$ with generator matrix of the form

$$\begin{bmatrix} B_{0a} & B_{0.a-1} & \cdots & B_{03} & B_{02} & B_{01} & I \\ pB_{1a} & pB_{1.a-1} & \cdots & pB_{13} & pB_{12} & pI & 0 \\ p^2B_{2a} & p^2B_{2.a-1} & \cdots & p^2B_{23} & p^2I & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ p^{a-1}B_{a-1.a} & p^{a-1}I & \cdots & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3}$$

where the column blocks have the same sizes as in (1). The dual code therefore contains $p^{k_\perp}$ codewords, where

$$k_\perp = \sum_{i=1}^{a} i k_i,$$

and has type

$$1^{k_a} p^{k_{a-1}} (p^2)^{k_{a-2}} \cdots (p^{a-1})^{k_1}. \tag{4}$$

Also $|C||C^\perp| = p^{k+k_\perp} = p^{an}$, and $(C^\perp)^\perp = C$.

Similarly, a nonzero linear code C over $\mathbb{Z}_{p^\infty}$ has a generator matrix which can be written in the form

$$G = \begin{bmatrix} p^{m_0}I & p^{m_0}A_{01} & p^{m_0}A_{02} & \cdots & p^{m_0}A_{0.b-1} & p^{m_0}A_{0.b} \\ 0 & p^{m_1}I & p^{m_2}A_{12} & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & p^{m_{b-1}}I & p^{m_{b-1}}A_{b-1.b} \end{bmatrix}, \tag{5}$$

where $0 \le m_0 < m_1 < \cdots m_{b-1}$, for some integer b, the column blocks have sizes k_0, $k_1, \ldots, k_b$ and the k_i are nonnegative integers adding to n. This means that C consists of all codewords

$$[v_0 \ v_1 \ v_2 \ \cdots \ v_b]G,$$

where each v_i is a vector of length k_i with components from $\mathbb{Z}_{p^\infty}$. We say that C has type

$$(p^{m_0})^{k_0} (p^{m_1})^{k_1} \cdots (p^{m_{b-1}})^{k_{b-1}}. \tag{6}$$

Now the code contains infinitely many codewords (although it is still finitely generated).

If $m_0 > 0$ in (5), all the codewords are multiples of p^{m_0}, and (since $\mathbb{Z}_{p^\infty}$ has characteristic 0) we may divide the whole code by p^{m_0}. We shall therefore usually only consider codes

in which $m_0 = 0$. In this case the dual code has a generator matrix similar to (3), with type

$$1^{k_b}(p^{m_1})^{k_{b-1}} \cdots (p^{m_{b-1}})^{k_1}, \tag{7}$$

and $(C^\perp)^\perp = C$. (If $m_0 > 0$ then $(C^\perp)^\perp = p^{-m_0}C$.)

The *automorphism group* $Aut(C)$ of a linear code C over $\mathbb{Z}_q$ is defined to be the set of all monomial matrices over $\mathbb{Z}_q$ that preserve the code. Since it contains all scalar matrices uI, where u is a unit in $\mathbb{Z}_q$, this group is infinite if $q = p^\infty$. We therefore define the *projective automorphism group* to be the quotient group $Aut(C)/\{uI : u = \text{unit}\}$.

A *cyclic* code C of length n over $\mathbb{Z}_q$ ($q = p^a$, $1 \le a \le \infty$) is a linear code with the property that if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(c_1, c_2, \ldots, c_{n-1}, c_0) \in C$. We assume throughout that n and p are relatively prime. As usual we represent codewords by polynomials, so cyclic codes are precisely the ideals in the ring

$$\mathcal{R} = \mathbb{Z}_q[X]/(X^n - 1).$$

3. Rings

We now discuss the properties of the ring $\mathcal{R}$ and of certain Galois rings $GR(q^m)$.

Let $q = p^a$ ($1 \le a \le \infty$), and let $\pi_1(X) \in \mathbb{Z}_p[X]$ be a monic primitive irreducible polynomial of degree m, so that $\pi_1(X)$ divides $X^n - 1 \bmod p$, where $n = p^m - 1$. The following are straightforward generalizations of results given in [16], [19], [27]. There is a unique monic irreducible polynomial $\pi_a(X) \in \mathbb{Z}_q[X]$ such that $\pi_a(X) \equiv \pi_1(X) \bmod p$ and $\pi_a(X)$ divides $X^n - 1$ over $\mathbb{Z}_q$ (see Theorem 1 below).

Let ξ be a root of $\pi_a(X)$, so that $\xi^n = 1$. Then the *Galois ring* $GR(q^m)$ is by definition the ring $\mathbb{Z}_q[\xi]$. There are two canonical ways to represent the elements of this ring. In the first representation, every element has a unique expansion

$$u = u_0 + pu_1 + p^2u_2 + \cdots + p^{a-1}u_{a-1}$$

(an infinite sum if $a = \infty$), where $u_i \in \mathcal{J} = \{0, 1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. The map $\tau : u \mapsto u_0$ is given by

$$\tau(u) = u^{p^m}, \quad u \in \mathbb{Z}_q[\xi],$$

and satisfies

$$\tau(uv) = \tau(u)\tau(v), \quad u, v \in \mathbb{Z}_q[\xi].$$

In the second representation u is written as

$$u = \sum_{r=0}^{n-1} v_r \xi^r, \quad v_r \in \mathbb{Z}_q.$$

The *Frobenius map* ϕ from $\mathbb{Z}_q[\xi]$ to $\mathbb{Z}_q[\xi]$ takes

$$\sum_{r=0}^{a-1} p^r u_r \quad \text{to} \quad \sum_{r=0}^{a-1} p^r u_r^p.$$

Then ϕ generates the Galois group of $\mathbb{Z}_q[\xi]$ over $\mathbb{Z}_q$, and ϕ^m is the identity map.

The following theorem plays a central role in studying cyclic codes over $\mathbb{Z}_q$. It shows that the irreducible factors of $X^n - 1$ over $\mathbb{Z}_q$ are in one-to-one correspondence with the factors over $\mathbb{Z}_p$.

THEOREM 1 *Let $q = p^a$, $1 \le a \le \infty$. If $h_1(X) \in \mathbb{Z}_p[X]$ is a monic irreducible divisor of $X^n - 1$ over $\mathbb{Z}_p$, then there is a unique monic irreducible polynomial $h_a(X) \in \mathbb{Z}_q[X]$ which divides $X^n - 1$ over $\mathbb{Z}_q$ and is congruent to $h_1(X)$ mod p.*

Proof. This result can be obtained from Hensel's Lemma, but we prefer to sketch a constructive proof (by induction).

For $1 \le r < \infty$, suppose $h_r(X) \in \mathbb{Z}_{p^r}[X]$ is a monic irreducible polynomial such that $h_r(X) \equiv h_1(X) \bmod p$, and $h_r(X) \mid X^n - 1$ over $\mathbb{Z}_{p^r}$. We will show that $h_r(X)$ can be lifted uniquely to a monic irreducible polynomial $h_{r+1}(X) \in \mathbb{Z}_{p^{r+1}}[X]$ which divides $X^n - 1$ over $\mathbb{Z}_{p^{r+1}}$. Then $h_\infty(X)$ is defined as the (p-adic) limit of $h_r(X)$ as $r \to \infty$.

Let $h(X) \in \mathbb{Z}_{p^{r+1}}[X]$ be any lift of $h_r(X)$, say $h(X) = h_r(X) + p^r g(X)$, and let α be a root of $h_r(X)$ and β a corresponding root of $h(X)$, so that $\beta = \alpha + p^r\delta$. Then

$$\begin{aligned} \alpha^n &= 1 + p^r\epsilon, \quad \beta^p = (\alpha + p^r\delta)^p = \alpha^p, \\ \beta^{np} &= (1 + p^r\epsilon)^p = 1. \end{aligned}$$

Therefore the monic polynomial whose roots are the p-th powers of the roots of $h(X)$ divides $X^n - 1$, and mod p^r has the same roots as $h_r(X)$, and so may be taken as $h_{r+1}(X)$. This polynomial is irreducible since its roots form one orbit under the Frobenius map. To show that $h_{r+1}(X)$ is unique, we argue as follows. Let $h(X)$ and $h'(X)$ be two different possibilities for $h_{r+1}(X)$, and let β and γ be zeros of h and h' respectively, with $\beta \equiv \gamma \bmod p^r$, say $\beta = \gamma + p^r\delta$. Then $\beta^n = \gamma^n = 1$, $\beta^p = \gamma^p$, hence $(\beta/\gamma)^n = (\beta/\gamma)^p = 1$. Since n and p are relatively prime, $\beta = \gamma$, and so $h = h'$. ∎

We now investigate the structure of ideals in $\mathcal{R}$. The units in $\mathcal{R}$ are precisely the elements $u = \sum_{r=0}^{n-1} u_r X^r$, $u_r \in \mathbb{Z}_q$, such that at least one of the u_r is a unit in $\mathbb{Z}_q$. We denote the natural map from $\mathcal{R}$ to $\mathbb{Z}_p[X]/(X^n - 1)$ by μ.

If $\mathcal{A}$ is an ideal in $\mathcal{R}$ with generators $f_1, f_2, \ldots$, we write $\mathcal{A} = (f_1, f_2, \ldots)$. The radical $Rad(\mathcal{A})$ of $\mathcal{A}$ is the set of all elements of $\mathcal{R}$, some power of which is in $\mathcal{A}$. The radical of the ideal $\{0\}$ is called the radical of $\mathcal{R}$, and denoted by $Rad(\mathcal{R})$. Then $Rad(\mathcal{R}) = (p)$ if $q = p^a$ is finite, or (0) if $q = p^\infty$.

The ring $\mathbb{Z}_{p^\infty}$ is a principal ideal domain, hence Noetherian. This implies that $\mathbb{Z}_{p^a}[X]$ and $\mathcal{R} = \mathbb{Z}_{p^a}[X]/(X^n - 1)$ are Noetherian for all $1 \le a \le \infty$. $\mathcal{R}$ satisfies the descending chain condition if $q = p^a$ is finite (since then $\mathcal{R}$ is finite), but not if $q = p^\infty$ (we will see examples later). Hence every maximal ideal in $\mathcal{R}$ is prime, and if q is finite every prime ideal different from (0) and (1) is maximal ([28], pp. 150, 203).

It is well-known that the prime ideals in $\mathbb{Z}_p[X]/(X^n - 1)$ are (0), (1) and (π_1), where π_1 is any monic irreducible divisor of $X^n - 1$ over $\mathbb{Z}_p$.

THEOREM 2 *If $q = p^a$ is finite the prime ideals in $\mathcal{R}$ are* (0), (1) *and* (π_a, p), *where π_a is any monic irreducible divisor of $X^n - 1$ over $\mathbb{Z}_q$. If $q = p^\infty$ there are in addition the prime (but nonmaximal) ideals* (π_a).

Proof. Let $\mathcal{A}$ be a prime ideal in $\mathcal{R}$ different from (0) and (1). Then $\mu(\mathcal{A}) = (\pi_1)$, say, so $\mathcal{A}$ contains π_a, where $\mu(\pi_a) = \pi_1$. If q is finite then $p \in \mathcal{A}$, or else $\mathcal{R}/\mathcal{A}$ would contain zero divisors, so $\mathcal{A} \supset (\pi_a, p)$, and it is easily seen that this ideal is maximal. If q is infinite and $p \notin \mathcal{A}$ then the only other possibility is $\mathcal{A} = (\pi_a)$. ∎

Note that the ideal (p) is not prime, since it contains the product of all the π_a—which is 0—but none of the π_a themselves.

It is also known that every ideal $\mathcal{A}$ in $\mathbb{Z}_p[X]/(X^n - 1)$ contains an idempotent e_1 (say), such that $\mathcal{A} = (e_1)$ ([18], Chapter 8, Theorem 1; [13], §24.2).

THEOREM 3 *Every prime ideal $\mathcal{A} = (\pi_a, p)$ in $\mathcal{R}$ contains an idempotent e_a with $e_a^2 = e_a$, $\mathcal{A} = (e_a, p)$. Furthermore, if q is infinite then every prime ideal $\mathcal{A} = (\pi_a)$ has an idempotent generator.*

Proof. We establish the first assertion by induction. Let (π_r, p) be the projection of $\mathcal{A}$ onto $\mathbb{Z}_{p^r}[X]/(X^n - 1)$, and suppose $e_r \in (\pi_r, p)$ is an idempotent with $(e_r, p) = (\pi_r, p)$. Then $e_r^2 = e_r + p^r h$ in $\mathbb{Z}_{p^{r+1}}[X]/(X^n - 1)$, for some h in $\mathbb{Z}_{p^{r+1}}[X]/(X^n - 1)$. If we take $e_{r+1} = e_r + p^r\theta$, then $e_{r+1}^2 - e_{r+1} = p^r(h - \theta(1 - 2e_r))$, and e_{r+1} is an idempotent in $\mathbb{Z}_{p^{r+1}}[X]/(X^n - 1)$ if we choose $\theta = h$ (if $p = 2$) or $\theta = h(1 - 2e_r)^{-1}$ (if $p > 2$). (Note that $(1 - 2e_r)^2 = 1 + 4p^r h$, so $1 - 2e_r$ is a unit.) It is easily verified that $(e_{r+1}, p) = (\pi_{r+1}, p)$. By repeating this process we obtain an idempotent $e_a \in \mathcal{A}$ with $(e_a, p) = (\pi_a, p)$.

To prove the second assertion, since π_a and $(X^n - 1)/\pi_a$ are relatively prime, we can find $h \in \mathbb{Z}_{p^\infty}[X]$ such that

$$h\pi_a - 1 \equiv 0 \mod (X^n - 1)/\pi_a,$$

so $h\pi_a(h\pi_a - 1) = 0$ in $\mathcal{R}$, and $h\pi_a$ is the desired idempotent. ∎

Next, every primary ideal is a power of a prime ideal.

THEOREM 4 *The primary ideals in $\mathcal{R}$ are* (0), (1), (π_a) *and* (π_a, p^i), *where π_a is an irreducible divisor of $X^n - 1$ over $\mathbb{Z}_q$ and $1 \le i < a$.*

We omit the proof. The key steps are (i) to show that if $\mathcal{A} = (\pi_a, p) = (e_a, p)$ is a prime ideal then

$$\mathcal{A}^i = (\pi_a, p)^i = (\pi_a, p^i) = (e_a, p^i), \tag{8}$$

for $1 \le i < a$, and (ii) to show that if $\mathcal{B}$ is a primary ideal whose associated prime ideal is $\mathcal{A} = (\pi_a, p)$ then (by [28], p. 200, Ex. 2) there is an integer j such that $\mathcal{A}^j \subseteq \mathcal{B} \subseteq \mathcal{A}$, and from this that $\mathcal{B} = \mathcal{A}^i$ for some i.

Note that when $q = p^a$ is finite then $(\pi_a, p)^a = (\pi_a)$, and

$$(\pi_a, p) \supset (\pi_a, p^2) \supset \cdots \supset (\pi_a, p^{a-1}) \supset (\pi_a)$$

is a finite descending sequence. When $q = p^\infty$, however,

$$(\pi_\infty, p) \supset (\pi_\infty, p^2) \supset (\pi_\infty, p^3) \supset \cdots \supset (\pi_\infty)$$

is an infinite descending sequence of primary ideals, the first and last of which are prime. In this case we adopt the convention that $(\pi_\infty, p)^\infty$ denotes (π_∞).

THEOREM 5 *Let $\pi_a^{(i)}$, $i = 1, \ldots, A$, denote the distinct monic irreducible divisors of $X^n - 1$ over $\mathbb{Z}_q$. Any ideal in $\mathcal{R}$ can be written in a unique way as*

$$\mathcal{A} = \prod_{i=1}^{A} (\pi_a^{(i)}, p)^{m_i}, \tag{9}$$

where $0 \le m_i \le a$. In particular if a is finite there are $(a+1)^A$ distinct ideals.

This is a consequence of Theorem 4 and the Lasker-Noether decomposition theorem ([28], p. 209). The product symbol in (9) may also be replaced by an intersection symbol.

THEOREM 6 *If $q = p^a$, $1 \le a < \infty$, any ideal in $\mathcal{R}$ has the form*

$$(f_0, pf_1, p^2 f_2, \ldots, p^{a-1} f_{a-1}), \tag{10}$$

where the f_i are divisors of $X^n - 1$ satisfying

$$f_{a-1} \mid f_{a-2} \mid \cdots \mid f_1 \mid f_0. \tag{11}$$

If $q = p^\infty$, any ideal in $\mathcal{R}$ has the form

$$(p^{m_0} f_0, p^{m_1} f_1, \ldots, p^{m_{b-1}} f_{b-1}), \tag{12}$$

where $0 \le m_0 < m_1 < \cdots < m_{b-1}$, for some b, and

$$f_{b-1} \mid f_{b-2} \mid \cdots \mid f_1 \mid f_0.$$

Proof. This follows by expanding the product in (9) and using (8). ∎

COROLLARY *Every ideal in $\mathcal{R}$ is principal.*

Proof. (i) If $q = p^a$, $1 \le a < \infty$, then the ideal defined by (10) has the generator

$$g = f_0 + pf_1 + p^2 f_2 + \cdots + p^{a-1} f_{a-1}.$$

We prove this for $a = 2$ and 3, leaving the general case to the reader. Let $\widehat{f_0} = (X^n - 1)/f_0$, $\widehat{f_i} = f_{i-1}/f_i$ for $1 \le i < a$. Case $a = 2$: Then $g = f_0 + pf_1$, and (g) contains

$pg = pf_0 = pf_1\hat{f}_1$ and $\hat{f}_0 g = pf_1\hat{f}_0$, hence pf_1 (since $\hat{f}_0$ and $\hat{f}_1$ have no common factors), hence f_0. Case $a = 3$: Now $g = f_0 + pf_1 + p^2 f_2$, and (g) contains $p^2 g = p^2 f_2 \hat{f}_1 \hat{f}_2$, $p\hat{f}_0 g = p^2 f_2 \hat{f}_0 \hat{f}_2$, and $\hat{f}_0 \hat{f}_1 g = p^2 f_2 f_0 \hat{f}_1$, hence $p^2 f_2$, hence $f_0 + pf_1$. So $(g) = (f_0 + pf_1, p^2 f_2)$. Arguing as in case $a = 2$ it follows that $(g) = (f_0, pf_1, p^2 f_2)$.

(b) Suppose $q = p^\infty$. Let g_a be a generator for the principal ideal given by the projection of the ideal onto $\mathbb{Z}_{2^a}$, for $a = 1, 2, \ldots$. Since $\mathcal{R}$ is compact in the p-adic metric, the sequence $\{g_a\}$ has a subsequence which converges to a limit g (say). Then g generates the ideal. ■

Finally, although we have not made any use of this, it is worth noting that $\mathcal{R}$ has a decomposition into a direct product of Galois rings:

$$\mathbb{Z}_{p^a}[X]/(X^n - 1) \cong \prod_{i=1}^{A} \mathbb{Z}_{p^a}[X]/(\pi_a^{(i)}).$$

4. Generalizations of Classical Codes to $\mathbb{Z}_q$

Theorem 1 provides a mechanism for generalizing any class of cyclic codes from $GF(p)$ to $\mathbb{Z}_{p^a}$ (for finite a) and even to the p-adic integers $\mathbb{Z}_{p^\infty}$. For example we define a *BCH code* of length n over $\mathbb{Z}_q$ ($q = p^a$, $1 \le a \le \infty$) to be the cyclic code whose generator polynomial is obtained by lifting the generator polynomial for a BCH code over $GF(p)$ to $\mathbb{Z}_q$. The resulting polynomial has a string of consecutive roots in the appropriate Galois ring $GF(q^m)$. (For finite q this is essentially the same as Shankar's [22] definition of BCH codes over $\mathbb{Z}_q$.) The code has type 1^k, where k is the dimension of the BCH code over $GF(p)$. One of the main unsolved questions here is to determine how the minimal Lee distance of these BCH codes varies as $a \to \infty$. (Similar questions can be asked about all the codes in this section.) We investigate the first nontrivial case of these BCH codes later in this section.

We define *Reed-Muller codes* (since they are extended cyclic codes [1], [18]) and *quadratic-residue codes* over $\mathbb{Z}_q$ in an analogous way.

If C is a code of length n over $\mathbb{Z}_q$ with generator matrix (1) or (5) and type (2) or (6), we define k by

$$k = \sum_{i=0}^{a-1} k_i \text{ (for (2))}, \quad \sum_{i=0}^{b-1} k_i \text{ (for (6))}.$$

The usual argument ([18], Chapter 2) then gives the Singleton bound:

$$d \le n - k + 1, \tag{13}$$

where d is the minimal Hamming distance of the code. We say that C is *maximal distance separable*, or MDS, if equality holds in (13). Since codes over $\mathbb{Z}_{p^\infty}$ have infinitely many codewords, it is better to use the equivalent definition (see [18], Chapter 11, Corollary 3) that a code is MDS if and only if every k columns of the generator matrix are linearly independent over $\mathbb{Z}_q$.

EXAMPLE 1 The 2-adic Hamming code of length 7. *In the binary case, $X^n - 1$ factors trivially over $\mathbb{Z}_q$, $q = 2^a$, $1 \le a \le \infty$, for $n = 1, 3$ and 5. The first nontrivial factorization is for $n = 7$, where it is easy[2] to find the 2-adic factorization*

$$X^7 - 1 = (X - 1)(X^3 + \lambda X^2 + (\lambda - 1)X - 1)(X^3 - (\lambda - 1)X^2 - \lambda X - 1), \quad (14)$$

where

$$\lambda = 0 + 2 + 4 + 32 + 128 + 256 + \cdots \quad (15)$$

is a 2-adic number satisfying

$$\lambda^2 - \lambda + 2 = 0. \quad (16)$$

The first 32 terms in the 2-adic expansion (15) of λ are

$$01100101111110011100110110000110\ldots. \quad (17)$$

There is no pattern to these digits.

Then the 2-adic code of length 7 and type 1^4 with generator polynomial

$$X^3 + \lambda X^2 + (\lambda - 1)X - 1$$

is the 2-adic lift of the familiar binary [7, 4] Hamming code. The generator polynomials for the versions of this code over $\mathbb{Z}_2, \mathbb{Z}_4, \ldots$ are:

$$\begin{aligned} \mathbb{Z}_2 &: X^3 + X + 1 \\ \mathbb{Z}_4 &: X^3 + 2X^2 + X - 1 \\ \mathbb{Z}_8 &: X^3 - 2X^2 - 3X - 1 \\ \mathbb{Z}_{16} &: X^3 + 6X^2 + 5X - 1 \\ \mathbb{Z}_{32} &: X^3 + 6X^2 + 5X - 1 \\ &\ldots \end{aligned} \quad (18)$$

(The coefficients can be read off (15).) By appending a 1 to the generating vectors of these codes, we obtain a sequence $\mathcal{H}_2, \mathcal{H}_4, \mathcal{H}_8, \ldots, \mathcal{H}_\infty$ of self-dual codes. In particular,

0	1	2	3	4	5	6	∞
1	λ	$\lambda - 1$	-1	0	0	0	1
0	1	λ	$\lambda - 1$	-1	0	0	1
0	0	1	λ	$\lambda - 1$	-1	0	1
0	0	0	1	λ	$\lambda - 1$	-1	1

(19)

is the generator matrix for a self-dual 2-adic code $\mathcal{H}_\infty$ of length 8 and type 1^4 that we call the *2-adic Hamming code*. This is in some sense the smallest interesting 2-adic code.

The $\mathbb{Z}_2$ version of this code, $\mathcal{H}_2$, is the [8, 4] Hamming code, and the $\mathbb{Z}_4$ version, $\mathcal{H}_4$, is the *octacode*, studied in [11], [12], [14], [16], and equivalent to the binary nonlinear Nordstrom-Robinson code.

The minimal Hamming and Lee distances of these codes are as follows:

	$\mathcal{H}_2$	$\mathcal{H}_4$	$\mathcal{H}_8$	$\mathcal{H}_{16}$	$\mathcal{H}_{32}$	$\mathcal{H}_{64}$	$\cdots$
Hamming	4	4	4	4	4	4	$\cdots$
Lee	4	6	8	12	14	18	$\cdots$

The minimal Hamming distance of $\mathcal{H}_{2^a}$ for $1 \le a < \infty$ is always 4, since the codeword obtained by multiplying any of the generators by 2^{a-1} has Hamming weight 4. However it follows from Theorem 8 below that the 2-adic Hamming code $\mathcal{H}_\infty$ has minimal Hamming distance 5, and is an MDS code.

On the other hand the sequence of Lee distances of these codes, 4, 6, 8, 12, 14, 18, ..., approaches infinity as $a \to \infty$. Unfortunately it appears that this sequence does not converge 2-adically, so one obvious definition of the minimal Lee distance of $\mathcal{H}_\infty$ fails. Even the Lee weight of the projections of the integer λ onto $\mathbb{Z}_{2^m}$ do not converge 2-adically as $m \to \infty$. For let $\lambda = \sum_{i=0}^{\infty} \lambda_i 2^i$ (the λ_i are given in (15), (18)), so the projection onto $\mathbb{Z}_{2^m}$ is $\alpha_m = \sum_{i=0}^{m-1} \lambda_i 2^i$, $m \ge 1$. The Lee weight of α_m is $w_m = \min\{\alpha_m, 2^m - \alpha_m\}$, and one can show that

$$w_m = (1 - 2\lambda_{m-1})\alpha_{m-1} + \lambda_{m-1}2^{m-1}, \quad m \ge 2.$$

This shows that $\{w_1, w_2, \ldots\} = \{0, 2, 2, 6, 6, 26, \ldots\}$ does not converge 2-adically.

There are several other natural ways to define the minimal distance of this code, but none are completely satisfactory. This is a question that requires further investigation.

The automorphism group of $\mathcal{H}_\infty$ contains operations corresponding to $x \mapsto x + 1$, $x \mapsto 2x$ and $x \mapsto -1/x$, namely the monomials

$$(0, 1, 2, 3, 4, 5, 6)(\infty),$$
$$(0)(1, 2, 4)(3, 6, 5)(\infty),$$
$$(0, \infty)(1, 6)(2, 3)(4, 5) \text{ \& negate } 0, 1, 2, 4,$$

which generate the central product $\mathbb{Z}_2.PSL_2(7)$, as well as all scalar matrices uI, $u =$ unit in $\mathbb{Z}_{2^\infty}$. Then the full projective automorphism group of $\mathcal{H}_\infty$ is $PSL_2(7)$, of order 168.

EXAMPLE 2 The 2-adic Golay code of length 24. *The binary Golay code can be lifted in a similar way. The factorization of* $X^{23} - 1$ *over* $\mathbb{Z}_{2^\infty}$ *is*

$$X^{23} - 1 = (X - 1)\pi_\infty^{(1)}(X)\pi_\infty^{(2)}(X),$$

where

$$\begin{aligned}\pi_\infty^{(1)}(X) \;=\; & X^{11} + \nu X^{10} + (\nu - 3)X^9 - 4X^8 - (\nu + 3)X^7 \\ & -(2\nu + 1)X^6 - (2\nu - 3)X^5 - (\nu - 4)X^4 + 4X^3 \\ & +(\nu + 2)X^2 + (\nu - 1)X - 1, \end{aligned} \tag{20}$$

$$\nu = 0 + 2 + 8 + 32 + 64 + 128 + \cdots \tag{21}$$

is a 2-adic number satisfying

$$\nu^2 - \nu + 6 = 0, \tag{22}$$

and $\pi_\infty^{(2)}(X)$ *is the reciprocal polynomial to* $\pi_\infty^{(1)}(X)$. *The first 32 terms in the 2-adic expansion (21) are*

$$01010111100100101100100001100000\ldots.$$

Then the cyclic code generated by $\pi_\infty^{(1)}(X)$, *extended by appending a 1 to the generators, is a self-dual 2-adic code* $\mathcal{G}_\infty$ *of length 24 and type* 1^{12}, *the* 2-adic Golay code. *The full projective automorphism group of* $\mathcal{G}_\infty$ *is* $PSL_2(23)$.

The projection on $\mathbb{Z}_2$ of $\mathcal{G}_\infty$ is the binary Golay code $\mathcal{G}_2$ of length 24 and minimal Hamming distance 8, and in fact every projection $\mathcal{G}_{2^a}$ of this code onto $\mathbb{Z}_{2^a}$ for finite a has minimal Hamming distance 8. However it follows from Theorem 8 that the 2-adic Golay code $\mathcal{G}_\infty$ has minimal Hamming distance 13, and is an MDS code.

As in the previous example, the $\mathbb{Z}_4$ version of this code, $\mathcal{G}_4$, is especially interesting. Bonnecaze and Solé [7] have shown that by applying Construction A to this code, i.e. by taking all vectors in $\mathbb{Z}^{24}$ which project onto $\mathcal{G}_4$ modulo 4, one obtains the Leech lattice. This is one of the simplest constructions known for this lattice (cf. [11]).

EXAMPLE 3 The 3-adic Golay code of length 12. *We lift the ternary Golay code in the same way, using the irreducible divisor*

$$X^5 + \theta X^4 - X^3 + X^2 + (\theta - 1)X - 1$$

of $X^{11} - 1$ *over* $\mathbb{Z}_{3^\infty}$, *where*

$$\theta = 0 + 3 + 9 + 2.27 + 2.81 + \cdots$$

is a 3-adic number satisfying

$$\theta^2 - \theta + 3 = 0. \tag{23}$$

By appending a 1 to each generator we obtain a self-dual 3-adic code $\mathcal{T}_\infty$ *of length 12 and type* 1^6, *the* 3-adic Golay code. *This has minimal Hamming distance 7 and is an MDS code. Its full projective automorphism group is* $PSL_2(11)$.

EXAMPLE 4 Binary quadratic residue codes. *Examples 1 and 2 may be generalized as follows. Let n be a prime of the form* $8m - 1$, *so that* $X^n - 1$ *factorizes over* $\mathbb{Z}_2$ *into* $(X - 1)\pi_2^{(1)}(X)\pi_2^{(2)}(X)$, *where all the factors are irreducible, with a corresponding factorization* $(X - 1)\pi_\infty^{(1)}(X)\pi_\infty^{(2)}(X)$ *over* $\mathbb{Z}_{2^\infty}$. *Let Q and N denote the nonzero quadratic residues and nonresidues modulo n, and set*

$$f_Q(X) = \sum_{i \in Q} X^i, \quad f_N(X) = \sum_{i \in N} X^i.$$

Then as in the binary case there are two inequivalent 2-adic quadratic residue codes of length n.

THEOREM 7 *The two quadratic residue codes of prime length $n = 8m - 1$ over $\mathbb{Z}_{2^\infty}$ have generator polynomials $\pi_\infty^{(1)}$ and $(X-1)\pi_\infty^{(1)}(X)$, and idempotents*

$$\alpha 1 + \beta f_Q(X) + \gamma f_N(X),$$

where the coefficients α, β, γ are the 2-adic numbers

$$\alpha = \frac{n+1}{2n}, \quad \beta = \frac{1+\sqrt{-n}}{2n}, \quad \gamma = \frac{1-\sqrt{-n}}{2n}$$

for the first code, and

$$\alpha = \frac{n-1}{2n}, \quad \beta = \frac{-1+\sqrt{-n}}{2n}, \quad \gamma = \frac{-1-\sqrt{-n}}{2n}$$

for the second code. By appending $\sqrt{\frac{-1}{n}}$ to each generator of the first code we obtain a self-dual code of length $n+1$ and type $1^{(n+1)/2}$.

We omit the straightforward proof, which includes the verification that when $n = 7$ and 23 the codes generated by $\pi_\infty^{(1)}(X)$ coincide with those constructed in Examples 1 and 2. The full projective automorphism group of the self-dual code of length $n+1$ is $PSL_2(n)$.

THEOREM 8 *The self-dual extended quadratic residue code of length $n+1$ described in Theorem 7 has minimal Hamming distance $(n+3)/2$, and is an MDS code.*

Proof. It follows from Blahut [4] that this code consists of all vectors $(c_0, c_1, \ldots, c_{n-1}, c_\infty) \in \mathbb{Z}_{2^\infty}^{n+1}$ that satisfy

$$\sqrt{\frac{-1}{n}} \sum_{j=0}^{n-1} c_j + c_\infty = 0,$$

$$\sum_{j=0}^{n-1} c_j \xi^{jq} = 0, \quad q \in Q,$$

where $\xi = e^{2\pi i/n}$. The usual Vandermonde argument then shows that this is an MDS code ∎

EXAMPLE 5 Cyclic codes of length 7 over $\mathbb{Z}_4$ and $\mathbb{Z}_{2^\infty}$. *As an illustration of the structure theorems of Section 3 (and also because one of them is the octacode) we enumerate the cyclic codes of length 7 over $\mathbb{Z}_4$. We factorize $X^7 - 1$ over $\mathbb{Z}_4$ from (14), obtaining*

$$(X-1)(X^3+2X+X-1)(X^3-X^2+2X-1) = f_0 f_1 f_2 \tag{24}$$

(say). The nontrivial prime ideals are, from Theorem 2,

$$P_0 = (f_0, 2), \quad P_1 = (f_1, 2), \quad P_2 = (f_2, 2),$$

Table 1. Cyclic (and extended cyclic) codes of length 7 over $\mathbb{Z}_4$. Number 12 is the octacode.

#	generators	type	ideal	$d(d^*)$
1	0000000 (0)	1^0	$0 = P_0^2P_1^2P_2^2$	-(-)
2	2222222 (2)	2^1	$(2f_1f_2) = P_0P_1^2P_2^2$	14 (16)
3	2220200 (0)	2^3	$(2f_0f_1) = P_0^2P_1^2P_2$	8(8)
5	2022000 (2)	2^4	$(2f_1) = P_0P_1^2P_2$	6(8)
7	2200000 (0)	2^6	$(2f_0) = P_0^2P_1P_2$	4(4)
8	2000000 (2)	2^7	$(2) = P_0P_1P_2$	2(4)
9	1000000 (1)	1^7	$(1) = 1$	1(2)
10	1300000 (0)	1^6	$(f_0) = P_0^2$	2(2)
11	1300000 (0), 2000000 (0)	1^62^1	$(f_0, 2) = P_0$	2(2)
12	1213000 (1)	1^4	$(f_1) = P_1^2$	4(6)
14	1213000 (1), 2000000 (0)	1^42^3	$(f_1, 2) = P_1$	2(4)
16	1132100 (0)	1^3	$(f_0f_1) = P_0^2P_1^2$	6(6)
18	1132100 (0), 2000000 (0)	1^32^4	$(f_0f_1, 2) = P_0P_1$	2(4)
20	1132100 (0), 2200000 (0)	1^32^3	$(f_0f_1, 2f_0) = P_0^2P_1$	4(4)
22	1132100 (0), 2022000 (2)	1^32^1	$(f_0f_1, 2f_1) = P_0P_1^2$	4(6)
24	1111111 (1)	1^1	$(f_1f_2) = P_1^2P_2^2$	7(8)
25	1111111 (1), 2000000 (0)	1^12^6	$(f_1f_2, 2) = P_1P_2$	2(4)
26	1111111 (1), 2022000 (0)	1^12^3	$(f_1f_2, 2f_1) = P_1^2P_2$	6(8)

and the other primary ideals are

$$P_0^2 = (f_0), \quad P_1^2 = (f_1), \quad P_2^2 = (f_2).$$

There are 27 codes, by Theorem 5, and they are displayed in Table 1 (except that we have omitted codes 4, 6, ..., 27, *which are equivalent to codes* 3, 5, ..., 26 *under the symmetry interchanging* f_1 *and* f_2*). The fourth column gives the canonical forms for these codes as described in Theorems 5 and 6.*

In Examples 1–4 we extended the codes to length $n + 1$ by appending a symbol that made them self-dual. For the codes in Table 1 it is more appropriate to append a zero-sum check symbol. The two extensions agree in the case of the octacode, which is number 12. The second column gives representative generators for the cyclic code (with the extending symbol in parentheses). The last column gives the minimal Lee distance d of the cyclic code (and the minimal distance d^* of the extended code in parentheses).

It is easy to extend this table to obtain a list of all possible types of cyclic codes over length n over $\mathbb{Z}_q$, $q = p^a$, $1 \le a \le \infty$, for any prime p such that $X^n - 1$ factorizes modulo p into three irreducible factors, as in (24). It follows from Theorem 6 that there are 24 types of such codes, namely

$$(p^{m_0}g_0), \quad (p^{m_0}g_0, p^{m_1}),$$

where $g_0 \in \{f_0, f_1, f_2, f_0f_1, f_0f_2, f_1f_2\}$, and

$$(p^{m_0}g_0, p^{m_1}g_1), \quad (p^{m_0}g_0, p^{m_1}g_1, p^{m_2}),$$

where $g_0 \in \{f_0f_1, f_0f_2, f_1f_2\}$, $g_1|g_0$, and

$$0 \leq m_0 < m_1 < m_2.$$

Similar enumerations can be obtained for any n, once the factorization of $X^n - 1$ is known.

Acknowledgements

We thank Mira Bernstein, Joe Buhler and especially John Conway for helpful conversations, and Christine Chang for assistance in tabulating cyclic codes over $\mathbb{Z}_4$.

Notes

1. This definition of type differs from the one given in [12], [16]. The present definition has the advantage that it applies also to p-adic codes.
2. Guided by the factorizations mod 2 and mod 4, one guesses that $X^6 + X^5 + \cdots + 1 = (X^3 + \lambda X^2 + \mu X - 1)\cdot$ reciprocal; hence $\mu = \lambda - 1$, $\lambda^2 = \lambda - 2$.

References

1. E. F. Assmus, Jr., and J. D. Key, *Designs and Their Codes*, Cambridge Univ. Press (1992).
2. E. F. Assmus, Jr., and H. F. Mattson, Jr., New 5-designs, *J. Combinat. Theory*, Vol. 6 (1969) pp. 122–151.
3. G. Bachman, *Introduction to p-Adic Numbers and Valuation Theory*, Academic Press, New York (1964).
4. R. E. Blahut, The Gleason-Prange theorem, *IEEE Trans. Inform. Theory*, Vol. 37 (1991) pp. 1269–1273.
5. I. F. Blake, Codes over certain rings, *Inform. Control*, Vol. 20 (1972) pp. 396–404.
6. I. F. Blake, Codes over integer residue rings, *Inform. Control*, Vol. 29 (1975) pp. 295–300.
7. A. Bonnecaze and P. Solé, Quaternary constructions of formally self-dual binary codes and unimodular lattices, *Lect. Notes Computer Sci.*, Vol. 781 (1994) pp. 194–206.
8. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York (1966).
9. G. Caire and E. Biglieri, Linear codes over cyclic groups, preprint, Sept., 1993.
10. A. R. Calderbank, *Topics in Algebraic Coding Theory*, Ph.D. dissertation, California Institute of Technology, Pasadena, Calif., 1980.
11. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 2nd edition (1993).
12. J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *J. Combinat. Theory*, Vol. A 62 (1993) pp. 30–45.
13. C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley (1962).
14. G. D. Forney, Jr., N. J. A. Sloane and M. Trott, The Nordstrom-Robinson code is the binary image of the octacode, in A. R. Calderbank et al. (eds.), *Coding and Quantization: DIMACS/IEEE Workshop 1992*, Amer. Math. Soc. (1993) pp. 19–26.
15. F. Q. Gouvêa, *p-adic Numbers*, Springer-Verlag, New York (1993).
16. A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, Vol. 40 (1994) pp. 301–319.
17. N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York (1977).
18. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1977).
19. B. R. McDonald, *Finite Rings with Identity*, Dekker, New York (1974).
20. D. W. Newhart, Information sets in quadratic residue codes, *Discrete Math.*, Vol. 42 (1982) pp. 251–266.
21. R. M. Roth and P. H. Siegel, A family of BCH codes for the Lee metric, preprint.

22. P. Shankar, On BCH codes over arbitrary integer rings, *IEEE Trans. Inform. Theory*, Vol. 25 (1979) pp. 480–483.
23. P. Solé, Open problem 2: cyclic codes over rings and p-adic fields, in G. Cohen and J. Wolfmann (eds.), *Coding Theory and Applications*, Lecture Notes in Computer Science, Springer-Verlag, New York, 388, (1988) p. 329.
24. E. Spiegel, Codes over $\mathbb{Z}_m$, *Inform. Control*, Vol. 35 (1977) pp. 48–51.
25. E. Spiegel, Codes over $\mathbb{Z}_m$, revisited, *Inform. Control*, Vol. 37 (1978) pp. 100–104.
26. S. K. Wasan, On codes over $\mathbb{Z}_m$, *IEEE Trans. Inform. Theory*, Vol. 28 (1982) pp. 117–120.
27. M. Yamada, Distance-regular digraphs of girth 4 over an extension ring of $\mathbb{Z}_4/4\mathbb{Z}_4$, *Graphs and Combinatorics*, Vol. 6 (1990) pp. 381–394.
28. O. Zariski and P. Samuel, *Commutative Algebra*, Van Nostrand, New York, Vol. I (1958).