Korean J. Math. **26** (2018), No. 3, pp. 537–544
https://doi.org/10.11568/kjm.2018.26.3.537

THE q-ADIC LIFTINGS OF CODES OVER FINITE FIELDS

Young Ho Park

Abstract. There is a standard construction of lifting cyclic codes over the prime finite field $\mathbb{Z}_p$ to the rings $\mathbb{Z}_{p^e}$ and to the ring of p-adic integers. We generalize this construction for arbitrary finite fields. This will naturally enable us to lift codes over finite fields $\mathbb{F}_{p^r}$ to codes over Galois rings $GR(p^e, r)$. We give concrete examples with all of the lifts.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of $q = p^r$ elements with characteristic p. A submodule of $\mathbb{F}_q^n$ is called a (linear) code of length n.

Let

$$GR(p^e, r) = \mathbb{Z}_{p^e}[X]/\langle h(X)\rangle \simeq \mathbb{Z}_{p^e}[\zeta],$$

where $h(X)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^e}[X]$ of degree r that divides $X^{p^r-1} - 1$. The polynomial $h(x)$ can be chosen so that $\zeta = X + \langle h(X)\rangle$ is a primitive $(p^r - 1)$st root of unity. $GR(p^e, r)$ is the Galois extension of degree r over $\mathbb{Z}_{p^e}$, called a *Galois ring*. Galois extensions are unique up to isomorphism. $GR(p^e, r)$ is a finite chain ring with ideals of the form $\langle p^i\rangle$ for $0 \le i \le e-1$, and residue field $\mathbb{F}_{p^r}$.

Received August 6, 2018. Revised September 10, 2018. Accepted September 12, 2018.

2010 Mathematics Subject Classification: 94B05, 11T71.

Key words and phrases: codes over rings, lifting, p-adic codes, Galois rings.

This work was supported by 2016 Research Grant from Kangwon National University (No. 520160208).

For generality on codes over fields, we refer [5,6]. See [2,7] for codes over $\mathbb{Z}_m$, and [2,3] for codes over p-adic rings.

Let $\mathbb{Q}_p$ denote the p-adic field and $\mathcal{O}_p$ its ring of integers. $\mathcal{O}_p$ is also denoted by $\mathbb{Z}_{p^\infty}$ at some literatures [1–3]. Cyclic codes over the prime field $\mathbb{Z}_p$ can be lifted to codes over $\mathbb{Z}_{p^e}$ and to the ring $\mathcal{O}_p$ [1]. A natural question to ask is therefore:

- Can we do the lifting for codes over general finite fields $\mathbb{F}_{p^r}$?

$$
\begin{array}{ccccccccc}
\mathbb{F}_{p^r} & \longleftarrow & ? & \longleftarrow & ? & \longleftarrow & \cdots & \longleftarrow & ? \\
\big\uparrow & & \big\uparrow & & \big\uparrow & & \big\uparrow & & \\
\mathbb{Z}_p & \longleftarrow & \mathbb{Z}_{p^2} & \longleftarrow & \mathbb{Z}_{p^3} & \longleftarrow & \cdots & \longleftarrow & \mathcal{O}_p
\end{array}
$$

Are there any rings corresponding to $\mathbb{Z}_{p^e}$ and $\mathcal{O}_p$?

2. Unramified extensions of $\mathbb{Q}_p$

We first review relevant facts on unramified extensions of p-adic fields.

THEOREM 2.1 ([4]). *Let $K/\mathbb{Q}_p$ be a finite extension of degree r. Then $|x| = \sqrt[r]{|N_{K/\mathbb{Q}_p}(x)|_p}$ is the unique non-archimedian absolute value on K extending the p-adic absolute value on $\mathbb{Q}_p$.*

The p-adic valuation on K is defined by

$$v_p(a) = -\log_p |a| \ (a \neq 0), \quad v_p(0) = 0$$

We define the valuation ring or ring of integers of K

$$\mathcal{O}_K = \{a \in K \mid |a| \leq 1\} = \{a \in K \mid v_p(a) \geq 0\}$$

and its maximal ideal

$$\mathcal{P}_K = \{a \in K \mid |a| < 1\} = \{a \in K \mid v_p(a) > 0\}.$$

The residue field of K is the quotient

$$\mathbb{K} = \mathcal{O}_K/\mathcal{P}_K.$$

We have the following results from [4].

THEOREM 2.2. *Let $K/\mathbb{Q}_p$ be a finite extension. Then*

1. $v_p(K) = \frac{1}{e}\mathbb{Z}$ for some positive divisor e of n.

2. $[\mathbb{K} : \mathbb{F}_p] = n/e$.

The number e is called the *ramification index* of K over $\mathbb{Q}_p$. A finite extension K of $\mathbb{Q}_p$ is said to be *unramified* if $e = 1$, i.e.,

$$\{|a| \mid a \in K\} = \{|a| \mid a \in \mathbb{Q}_p\} = \{p^v \mid v \in \mathbb{Z}\}$$

K is *ramified* if $e > 1$, totally ramified if $e = n$. For example, $\mathbb{Q}_5(\sqrt{2})$ is unramified, while $\mathbb{Q}_5(\sqrt{5})$ is ramified.

THEOREM 2.3 ([4]). *For each integer $r \geq 1$, there exists a unique unramified extension $\mathbb{Q}_{p^r}$ of degree r over $\mathbb{Q}_p$. It can be obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^r - 1)$st root of unity. In fact, $\mathbb{Q}_{p^r}$ contains all $(p^r - 1)$st root of unity.*

Here is how we construct $\mathbb{Q}_{p^r}$.

1. Let $\bar{\zeta}$ be a generator of $\mathbb{F}^*_{p^r}$. Then $\mathbb{F}_{p^r} = \mathbb{F}_p(\bar{\zeta})$.
2. Let $\bar{h}(X)$ be the minimal polynomial for $\bar{\zeta}$ over $\mathbb{F}_p$. Lift $\bar{h}(X)$ to any $h(X) \in \mathcal{O}_p[X]$ which is then an irreducible polynomial over $\mathcal{O}_p$ and $\mathbb{Q}_p$ of degree r.
3. If ζ is a root of $h(X)$, then $\mathbb{Q}_p(\zeta)$ is an extension of degree r.
4. If β is any $(p^r - 1)$st root of unity, then $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\zeta)$. Thus $\mathbb{Q}_p(\zeta) = \mathbb{Q}_{p^r}$.

The ring of integers of $\mathbb{Q}_{p^r}$ will be denoted by $\mathcal{O}_{p^r}$:

$$\mathcal{O}_{p^r} = \{a \in \mathbb{Q}_{p^r} \mid |a| \leq 1\}.$$

$\mathcal{O}_{p^r}$ is the set of all roots in $\mathbb{Q}_{p^r}$ of monic polynomials over $\mathcal{O}_p$.

THEOREM 2.4 ([4]). *$\mathcal{O}_{p^r} = \mathcal{O}_p[\zeta]$, where ζ is a primitive $(p^r - 1)$st root of unity.*

Its unique maximal ideal is

$$\mathcal{P}_{p^r} = (p) = \{a \in \mathbb{Q}_{p^r} \mid |a| < 1\}$$

and the residue field of $\mathbb{Q}_{p^r}$ is

$$\mathcal{O}_{p^r}/\mathcal{P}_{p^r} \simeq \mathbb{F}_{p^r}.$$

THEOREM 2.5 ([4]). *If $R = \{0, c_1, c_2, \cdots, c_{p^r-1}\}$ is a set of complete representatives of $\mathcal{O}_{p^r}/\mathcal{P}_{p^r}$, then every element of $\mathcal{O}_{p^r}$ can be written uniquely as*

$$a_0 + a_1 p + \cdots + a_t p^t + \cdots$$

where $a_i \in R$.

Theorem 2.6 (Hensel's Lemma v1). *Let $F(X) \in \mathcal{O}_{p^r}[X]$. Suppose that there exists an $\alpha_1 \in \mathcal{O}_{p^r}$ such that*

$$F(\alpha_1) \equiv 0 \pmod p, \quad F'(\alpha_1) \not\equiv 0 \pmod p$$

Then there exists a unique $\alpha \in \mathcal{O}_{p^r}$ such that $\alpha \equiv \alpha_1 \pmod p$ and $F(\alpha) = 0$.

Example 2.7. Consider $f(X) = X^2 - 2 \in \mathbb{Q}_5[X]$. It has a root $\bar{\alpha}$ in $\mathbb{F}_{25} = \mathcal{O}_{25}/\mathcal{P}_{25}$. Take $\alpha \in \bar{\alpha}$. Then $f(\alpha) \equiv 0 \pmod 5$ and $f'(\alpha) = 2\alpha \not\equiv 0 \pmod 5$. Therefore $X^2 - 2$ has a root in $\mathbb{Q}_{25}$. Similarly, $X^2 - 3$ has a root in $\mathbb{Q}_{25}$. We note that this implies $\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_{25} = \mathbb{Q}_5(\sqrt{3})$.

We can also see from Hensel's Lemma that the set of all $(p^r - 1)$st root of unity in $\mathcal{O}_{p^r}$ together with 0

$$T_r = \{0, 1, \zeta, \cdots, \zeta^{p^r-2}\}$$

is a complete set of coset representatives for $\mathcal{O}_{p^r}/(p)$.

3. Cyclic lifts

For each natural number e,

$$\mathcal{O}_{p^r}/(p^e) = \mathcal{O}_p[\zeta]/(p^e) = \mathbb{Z}_{p^e}[\zeta]/(p^e) = GR(p^e, r).$$

We have a projective systems

$$\begin{array}{ccccccccc}
\mathbb{F}_{p^{rs}} \simeq GR(p, rs) & \longleftarrow & GR(p^2, rs) & \longleftarrow & GR(p^3, rs) & \longleftarrow & \cdots & \longleftarrow & \mathcal{O}_{p^{rs}} \\
| & & | & & | & & & & | \\
\mathbb{F}_{p^r} \simeq GR(p, r) & \longleftarrow & GR(p^2, r) & \longleftarrow & GR(p^3, r) & \longleftarrow & \cdots & \longleftarrow & \mathcal{O}_{p^r} \\
| & & | & & | & & & & | \\
\mathbb{F}_p \simeq \mathbb{Z}_p & \longleftarrow & \mathbb{Z}_{p^2} & \longleftarrow & \mathbb{Z}_{p^3} & \longleftarrow & \cdots & \longleftarrow & \mathcal{O}_p
\end{array}$$

On each of extensions in two fixed rows, we have the isomorphic cyclic Galois groups:

$$\mathrm{Gal}(GR(p^e, rs)/GR(p^e, r)) \simeq \mathrm{Gal}(\mathcal{O}_{p^{rs}}/\mathcal{O}_{p^r})$$

generated by $\mathtt{Fr}^r$ determined by the property $\mathtt{Fr}^r(x) \equiv x^{p^r} \pmod p$. More precisely,

$$\mathtt{Fr}^r(a_0 + a_1 p + \cdots + a_t p^t + \cdots) = a_0^{p^r} + a_1^{p^r} p + \cdots + a_t^{p^r} p^t + \cdots$$

where $a_i \in T_r$. In particular, if α is any nth of unity in $\mathcal{O}_{p^{rs}}$, where $n \mid p^{rs} - 1$, then

$$\mathtt{Fr}^r(\alpha) = \alpha^{p^r}$$

THEOREM 3.1 (Hensel's Lemma v2). *Let $f(X) \in \mathcal{O}_{p^r}[X]$ and assume that there exist $g_1(X), h_1(X) \in \mathcal{O}_{p^r}[X]$ such that*

1. *$g_1(X)$ is monic*
2. *$g_1(X)$ and $h_1(X)$ are relatively prime modulo p*
3. *$f(X) \equiv g_1(X)h_1(X) \pmod{p}$*

Then there exist unique $g(X), h(X) \in \mathcal{O}_{p^r}$ such that

1. *$g(X)$ is monic (so $\deg g = \deg g_1$)*
2. *$g(X) \equiv g_1(X) \pmod{p}$, $h(X) \equiv h_1(X) \pmod{p}$*
3. *$f(X) = g(X)h(X)$.*

Proof. (Constructive proof) We construct inductively two sequences g_n and h_n such that

1. g_n is monic of the same degree as g_1
2. $g_{n+1} \equiv g_n \pmod{p^n}$, $h_{n+1} \equiv h_n \pmod{p^n}$
3. $f \equiv g_n h_n \pmod{p^n}$

We follow the following steps:

1. Assume g_n, h_n are constructed. Let $f - g_n h_n = p^n k_n$.
2. There are $a, b \in \mathcal{O}_{p^r}[X]$ such that $1 \equiv a g_n + b h_n \pmod{p}$, hence $k_n \equiv (a k_n) g_n + (b k_n) h_n \pmod{p}$.
3. Let $b k_n = g_n q_n + r_n$ with $\deg r_n < \deg g_n = \deg g_1$. Let $s_n = (a k_n) + h_n q_n$. Then $r_n h_n + s_n g_n \equiv k_n \pmod{p}$
4. Now set $g_{n+1} = g_n + p^n r_n$, $h_{n+1} = h_n + p^n s_n$. ($\deg g_{n+1} = \deg g_n$)
5. Then $f \equiv g_{n+1} h_{n+1} \pmod{p^{n+1}}$.

□

Since any cyclic code of length n over $\mathbb{F}_{p^r} = \mathcal{O}_{p^r}/(p)$ is generated by a monic factor $g_1(X)$

$$X^n - 1 = g_1(X)h_1(X)$$

of $X^n - 1$, Hensel's Lemma v2 provides a mechanism for generalizing any class of cyclic codes from $\mathbb{F}_{p^r}$ to $\mathcal{O}_{p^r}/(p^e) = GR(p^e, r)$ by

$$X^n - 1 \equiv g_e(X)h_e(X) \pmod{p^e}$$

and to $\mathcal{O}_{p^r}$ by

$$X^n - 1 = g(X)h(X)$$

4. Examples

We consider the case $q = 4 = 2^2$ so that $p = 2$ and $r = 2$. We have that

$$\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\} = \{0, 1, \omega, \omega^2\}$$

where ω is a root of the polynomial $\bar{h}(X) = X^2 + X + 1 \in \mathbb{F}_2[x]$ of degree 2 and that $\mathbb{F}_4 = \mathbb{F}_2(\omega)$. We lift $\bar{h}(X)$ to $\mathcal{O}_2$ as $h(X) = X^2 + X + 1$. This is irreducible over $\mathcal{O}_2$ and over $\mathbb{Q}_2$. Let ζ be a root of $h(X)$, so that $\mathbb{Q}_2(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}_2\}$ is the extension of degree 2. Since we may take $\zeta \equiv \omega \pmod 2$, we will replace ω with ζ. This way, we have that

$$\mathbb{F}_4 = \mathbb{F}_2[\zeta], \quad \mathcal{O}_4 = \mathcal{O}_2(\zeta), \quad \mathbb{Q}_4 = \mathbb{Q}_2[\zeta].$$

In general we will simply write ζ for $\zeta \pmod{p^e}$.

We will consider cyclic codes of length 11. First we compute the cyclotomic cosets mod $n = 11$ over $\mathbb{F}_4$ of s:

$$C_s = \{s, sq, sq^2, \cdots, sq^{m_s - 1}\}$$

where $sq^{m_s} \equiv 1 \pmod n$. In our case, we have three cosets

$$C_0 = \{0\}, \quad C_1 = \{1, 4, 5, 9, 3\}, \quad C_2 = \{2, 8, 10, 7, 6\}.$$

Thus $X^{11} - 1$ splits into linear factors in $\mathbb{F}_{4^5}$, where $5 = |C_1|$. Let $\alpha \in \mathbb{F}_{4^6}$ be a 11^{th} root of unity. Then $X^{11} - 1$ factors in $\mathbb{F}_4$ as

$$X^{11} - 1 = (X - 1)g(X)h(X)$$

where $g(X) = (X - \alpha)(X - \alpha^4)(X - \alpha^5)(X - \alpha^9)(X - \alpha^3)$ and $h(X) = (X - \alpha^2)(X - \alpha^8)(X - \alpha^{10})(X - \alpha^7)(X - \alpha^6)$ in $\mathbb{F}_4[X]$. Actually, we have that

$$\begin{aligned} g(X) &= X^5 + \zeta X^4 + X^3 + X^2 + \zeta^2 X + 1, \\ h(X) &= X^5 + \zeta^2 X^4 + X^3 + X^2 + \zeta X + 1. \end{aligned}$$

We will lift the cyclic code $\langle g(X) \rangle$ to $GR(2^e, 2)$, and hence we would like to find $g_e(X), h_e(X) \in GR(2^e, 2)[X] = \mathbb{Z}_{2^e}[\zeta][X]$ for all $e = 2, 3, \cdots$ such that $X^{11} - 1 = (X-1)g_e(X)h_e(X)$. We list first few lifts for $e = 2, 3, 4$:

$$\begin{aligned}
g_2(X) &= X^5 + (-\zeta + 2)X^4 - X^3 + X^2 + (-\zeta + 1)X - 1 \\
g_3(X) &= X^5 + (3\zeta - 2)X^4 - X^3 + X^2 + (3\zeta - 3)X - 1 \\
g_4(X) &= X^5 + (-5\zeta - 2)X^4 - X^3 + X^2 + (-5\zeta - 3)X - 1 \\
h_2(X) &= X^5 + (\zeta - 1)X^4 - X^3 + X^2 + (\zeta + 2)X - 1 \\
h_3(X) &= X^5 + (-3\zeta + 3)X^4 - X^3 + X^2 + (-3\zeta + 2)X - 1 \\
h_4(X) &= X^5 + (5\zeta + 3)X^4 - X^3 + X^2 + (5\zeta + 2)X - 1
\end{aligned}$$

From these lifts we conjecture that the q-adic lifts have the form

$$g_\infty(X) = X^5 + \lambda X^4 - X^3 + X^2 + (\lambda - 1)X - 1 \tag{1}$$

$$h_\infty(X) = X^5 + (1-\lambda)X^4 - X^3 + X^2 - \lambda X - 1 \tag{2}$$

for some $\lambda \in \mathcal{O}_4$. We must have that

$$g_\infty(X)h_\infty(X) = 1 + x + x^2 + \cdots + x^{10} \tag{3}$$

in $\mathcal{O}_4[X]$. By expanding $g_\infty(X)h_\infty(X)$ out with Equations (1) and (2), it is easy to see that Equation (3) is equivalent to

$$\lambda^2 - \lambda + 3 = 0. \tag{4}$$

Now we finally obtain the factorization $X^{11} - 1$ in $\mathcal{O}_4[X]$ as

$$X^{11} - 1 = (X-1)g_\infty(X)h_\infty(X).$$

Consequently, we can obtain all the cyclic lifts to $GR(2^e, 2)$ for all e by solving the Equation (4) modulo 2^e .

By the same method explained above, we found a list of factorizations of $x^n - 1$ for q-adic cyclic codes of small length n:

$$
\begin{aligned}
x^3 - 1 &= (x-1)(x-\zeta)(x-\zeta^2) \\
x^5 - 1 &= (x-1)(x^2+\lambda x+1)(x^2+(1-\lambda)x+1), \\
&\qquad\quad \text{where } \lambda^2-\lambda-1=0 \\
x^7 - 1 &= (x-1)(x^3+\lambda x^2+(\lambda-1)x-1)(x^3-(\lambda-1)x^2-\lambda x-1), \\
&\qquad\quad \text{where } \lambda^2-\lambda+2=0 \\
x^9 - 1 &= (x-1)(x-\zeta)(x+\zeta^2)(x^3-\zeta)(x^3+\zeta^2) \\
x^{13} - 1 &= (x-1)(x^6+\lambda x^5+2x^4+(\lambda-1)x^3+2x^2+\lambda x+1)\cdot \\
&\quad (x^6+(1-\lambda)x^5+2x^4-\lambda x^3+2x^2+(1-\lambda)x+1), \\
&\qquad\quad \text{where } \lambda^2-\lambda-3=0.
\end{aligned}
$$

These factorizations give the lifts of cyclic codes of odd lengths ≤ 13 to the Galois rings $GR(2^e, 2)$.

References

[1] A.R.Calderbank and N.J.A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes. Cryptogr. **6** (1995), 21–35.

[2] S.T. Dougherty, S.Y. Kim and Y.H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), 123–135.

[3] S.T. Dougherty and Y.H. Park, *Codes over the p-adic integers*, Des. Codes. Cryptogr. **39** (2006), 65–80.

[4] F. Q. Gouvêa, *p-adic numbers. An introduction*, Springer, 2003.

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003.

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

[7] Y.H. Park, *Modular independence and generator matrices for codes over* $\mathbb{Z}_m$, Des. Codes. Cryptogr. **50** (2009), 147–162.

Young Ho Park
Department of Mathematics
Kangwon National University
Chuncheon 24341, Korea
E-mail: `yhpark@kangwon.ac.kr`