ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 305 (2005) 123 – 135

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Lifted codes and their weight enumerators

Steven T. Dougherty[a], Sun Young Kim[b], Young Ho Park[b]

[a] *Department of Mathematics, University of Scranton, Scranton, PA 18510, USA*
[b] *Department of Mathematics, Kangwon National University, Chuncheon 200-701, Korea*

Received 15 March 2004; received in revised form 28 July 2005; accepted 17 August 2005

Abstract

We describe some structural results for codes over the rings $\mathbb{Z}_p$ and use them to examine lifts of codes over these rings to $\mathbb{Z}_{p^e}$ and to codes over the p-adics. We determine the weight enumerator of all lifts of the length 8 Hamming code and the length 12 ternary Golay code. We show that all weight enumerators of the lifts of the length 24 Golay code can be determined after a finite computation.

Keywords: Lifted codes; Weight enumerators; p-Adic codes; Minimum distance

1. Codes over $\mathbb{Z}_{p^e}$

Numerous interesting results have been found for codes over the rings $\mathbb{Z}_p$. In [1], Calderbank and Sloane investigated codes over the p-adics and examined lifts of codes over $\mathbb{Z}_p$ to $\mathbb{Z}_{p^e}$ and to the p-adics. In this work we continue this investigation and examine the weight enumerators and structures of these codes.

We begin with some definitions. Let p be a prime. A *linear* code C of length n over $\mathbb{Z}_{p^e}$ is a submodule of $\mathbb{Z}_{p^e}^n$. The (Hamming) *weight* $\mathrm{wt}(\mathbf{x})$ of a vector $\mathbf{x} = (x_i) \in \mathbb{Z}_{p^e}^n$ is the number of nonzero entries of $\mathbf{x}$ and the support of $\mathbf{x}$ is the set $\mathrm{supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$. The minimum distance $d(C)$ of a code C is the smallest weight among nonzero codewords in C. Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$. The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ are said to be modular independent if $\sum a_i \mathbf{v}_i = \mathbf{0}$ implies all a_i are nonunits, i.e., $p \mid a_i$ for all i.

E-mail addresses: doughertys1@scranton.edu (S.T. Dougherty), sykim@math.kangwon.ac.kr (S.Y. Kim), yhpark@kangwon.ac.kr (Y.H. Park).

0012-365X/$ - see front matter
doi:10.1016/j.disc.2005.08.004

A generator matrix for a code C over $\mathbb{Z}_{p^e}$ is permutation equivalent to a matrix of the form which we refer to as the standard form:

$$M=\begin{bmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \dots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \dots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2I_{k_2} & p^2A_{23} & \dots & p^2A_{2,e-1} & p^2A_{2e} \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & p^{e-1}I_{k_{e-1}} & p^{e-1}A_{e-1,e} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0I_{k_e} \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}, \tag{1}$$

where the columns are grouped into square blocks of sizes $k_0, k_1, \dots, k_{e-1}, k_e$ and the k_i are nonnegative integers adding to n.

Let C be a code. We say that the codewords $\mathbf{v}_1, \dots, \mathbf{v}_k$ form a basis of C if they are modular independent and generate C.

A matrix with a standard form in (1) is said to be of *type*

$$(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}0^{k_e}, \tag{2}$$

omitting terms with zero exponents, if any. Often the 0^{k_e} is left off the type, but we retain it since we use k_e later. The number of nonzero rows is called the *rank* of M and denoted by rank M. If the code is of type 1^k for some k then we say that the code is a free code.

The type and the rank of a code C are defined to be the type and the rank of its generator matrix. A code of length n with rank k is called an $[n, k]$ code, or $[n, k, d]$ code if we want to specify its minimum distance d. If C has the type $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}$ over $\mathbb{Z}_{p^e}$, then

$$|C| = (p^e)^{k_0}(p^{e-1})^{k_1}(p^{e-2})^{k_2}\cdots(p^1)^{k_{e-1}}. \tag{3}$$

The *dimension* of the code C over $\mathbb{Z}_{p^e}$ is defined by $\dim C = \log_{p^e}|C|$. Note that $\dim C$ is not necessarily an integer.

We say that a vector $\mathbf{v} \in C$ is said to be reduced if it contains an invertible element.

Definition 1.1. We define the inner product of $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ in C by

$$\mathbf{x}\cdot\mathbf{y} = x_1y_1 + \cdots + x_ny_n \pmod{p^e}.$$

The *dual code* $C^\perp$ of C is defined as

$$C^\perp = \{\mathbf{x} \in \mathbb{Z}_{p^e}^n \mid \mathbf{x}\cdot\mathbf{y} = 0 \text{ for all } \mathbf{y} \in C\}.$$

C is *self-dual* if $C = C^\perp$.

Now we shall consider codes over the infinite ring $\mathbb{Z}_{p^\infty}$ of p-adic integers. A linear code $\mathscr{C}$ of length n over $\mathbb{Z}_{p^\infty}$ is a submodule of the free module $\mathbb{Z}_{p^\infty}^n$. Note that $\mathbb{Z}_{p^\infty}$ is a principal ideal domain. First we recall a theorem on the finitely generated modules over a principal ideal domain.

Theorem 1.2. *Let R be a principal ideal domain, M be a free module of rank n over R and $\mathscr{C}$ be a submodule of M. Then*

(i) *$\mathscr{C}$ is a free module of rank $k \leqslant n$ and*
(ii) *there exists a basis $y_1, y_2, \ldots, y_n$ of M so that $d_1 y_1, d_2 y_2, \ldots, d_k y_k$ is a basis of $\mathscr{C}$, where d_i are nonzero elements of R with the divisibility relations $d_1 | d_2 | \cdots | d_k$.*

A code $\mathscr{C}$ of length n with rank k over $\mathbb{Z}_{p^\infty}$ is called a p-adic $[n, k]$-*code*. We call k the *dimension* of $\mathscr{C}$ and denote by $\dim \mathscr{C} = k$. A $k \times n$ matrix whose rows form a basis of $\mathscr{C}$ is called a *generator matrix* of $\mathscr{C}$. As in the case of $\mathbb{Z}_{p^e}$, G can be transformed into the standard form

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \ldots & A_{0,r-1} & A_{0r} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \ldots & pA_{1,r-1} & pA_{1r} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{23} & \ldots & p^2 A_{2,r-1} & p^2 A_{2r} \\ \cdot & \cdot & \cdot & \cdot & \ldots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \ldots & p^{r-1} I_{k_{r-1}} & p^{r-1} A_{r-1,r} \end{bmatrix}, \tag{4}$$

where the columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{r-1}, k_r = n - k$, the k_i are nonnegative integers with $\sum_{i=1}^{e} k_i = n$ and $k_{r-1} \neq 0$.

The innerproduct and the dual code are defined for p-adic codes as above except that the computations are done over $\mathbb{Z}_{p^\infty}$. As pointed out in [3], the dual of any p-adic $[n, k]$ code has type 1^{n-k}, and hence $(\mathscr{C}^\perp)^\perp \neq \mathscr{C}$ in general. If $\mathscr{C}^\perp = \mathscr{C}$, then $\mathscr{C}$ is called a self-dual code.

The following theorem is proven for codes over the p-adics in [1] and for codes over rings in [11].

Theorem 1.3. *Let $\mathscr{C}$ be either a p-adic $[n, k]$-code or a code over $\mathbb{Z}_{p^e}$ of length n then*

$$\dim \mathscr{C} + \dim \mathscr{C}^\perp = n.$$

In the next section we shall show how to determine weight enumerators and minimum weights of liftings of codes. In preprint [5] similar results are obtained about the weight enumerators of the liftings of codes over $\mathbb{Z}_{p^e}$, specifically they determine symmetrized weight enumerators for the lifted quadratic residue codes of length 24 modulo 2^m and 3^m for any positive m. In [9] similar results on the minimum weights of lifts are obtained, specifically they relate minimum weights and supports of minimum weight vectors for codes over a finite chain ring and codes over its residue field. They show that the minimum weight does not decrease for Hensel lifts of cyclic codes over the residue field.

2. Lifts of codes

Each element in the finite ring Z_{p^e} can be written uniquely as the finite sum

$$\sum_{i=0}^{e-1} a_i p^i = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_{e-1} p^{e-1}, \tag{5}$$

where $0\leqslant a_i < p$. Similarly any element in the ring $\mathbb{Z}_{p^\infty}$ can be written uniquely as the infinite sum

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots, \tag{6}$$

where $0\leqslant a_i < p$. Define a map $\Psi_e : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^e}$ by

$$\Psi_e\left(\sum_{i=0}^{\infty} a_i p^i\right) = \sum_{i=0}^{e-1} a_i p^i. \tag{7}$$

We use the same notation for the maps $\Psi_e = \Psi_e^f : \mathbb{Z}_{p^f} \to \mathbb{Z}_{p^e}$ defined by

$$\Psi_e\left(\sum_{i=0}^{f-1} a_i p_i\right) = \sum_{i=0}^{e-1} a_i p^i,$$

where $f\geqslant e$. Clearly Ψ_e is a ring homomorphism.

Definition 2.1. Let $1\leqslant e_1\leqslant e_2$ be integers. An $[n, k]$ code C_1 over $\mathbb{Z}_{p^{e_1}}$ *lifts* to an $[n, k]$ code C_2 over $\mathbb{Z}_{p^{e_2}}$, denoted by $C_1 \prec C_2$, if C_2 has a generator matrix G_2 such that $\Psi_{e_1}(G_2)$ is a generator matrix of C_1.

The proof of the following is straightforward.

Lemma 2.2. *Let M be a matrix over $\mathbb{Z}_{p^\infty}$. If M' is a standard form of M, then $\Psi_e(M')$ is a standard form of $\Psi_e(M)$.*

Therefore, for a p-adic $[n, k]$ code $\mathscr{C}$ of type 1^k, $\mathscr{C}^e = \Psi_e(\mathscr{C})$ is an $[n, k]$ code of type 1^k over $\mathbb{Z}_{p^e}$. In this work we are generally concerned with codes over $\mathbb{Z}_{p^e}$ that are projections of codes over the p-adics. As such, the codes we consider are free codes, that is codes of type 1^k.

Note that $\mathscr{C}^e \prec \mathscr{C}^{e+1}$ for all e. Thus if a code $\mathscr{C}$ over $\mathbb{Z}_{p^\infty}$ of type 1^k is given, then we obtain a series

$$\mathscr{C}^1 \prec \mathscr{C}^2 \prec \cdots \prec \mathscr{C}^e \prec \cdots$$

of lifts of codes. Conversely, let C be an $[n, k]$ code over $\mathbb{Z}_p$, and $G = G_1$ be its generator matrix. It is clear that we can define a series of generator matrices $G_e \in \mathrm{Mat}_{k\times n}(\mathbb{Z}_{p^e})$ such that $\Psi_e(G_{e+1}) = G_e$. This defines a series of lifts C_e of C to $\mathbb{Z}_{p^e}$ for all finite e. Then this series of lifts determines a unique p-adic code $\mathscr{C}$ such that $\mathscr{C}^e = C_e$. Therefore, a p-adic code of type 1^k represents a series of lifts from a code over $\mathbb{Z}_p$. Even self-dual codes can be lifted to self-dual codes. In fact, it is proven in [10] that any Type II binary self-dual code can be lifted to a self-dual code, and it is proven in [3] that any nonbinary self-dual code can be lifted to a self-dual code. For example, if $G_1 = (I|A_1)$ is a generator matrix of C, then $(I|A_{e+1})$ is a generator matrix of $C_{e+1} \succ C_e$, where

$$A_{e+1} = \left(\frac{p+3}{2} I + \frac{p+1}{2} A_e A_e^t \right) A_e.$$

For the rest of our paper, we consider only p-adic codes of type 1^k.

Let $\mathscr{C}$ be a p-adic $[n, k]$ code $\mathscr{C}$ of type 1^k, and G, H be a generator matrix and a parity-check matrix of $\mathscr{C}$, respectively, such that $GH^{\mathrm{T}} = 0$. Let $G_e = \Psi_e(G)$ and $H_e = \Psi_e(H)$. Then G_e, H_e are generator matrices and parity check matrices of $\mathscr{C}^e$, respectively, such that $G_e H_e^{\mathrm{T}} = 0$.

Lemma 2.3. *Let $f < e < \infty$.*

(i) $p^{e-f} G_f \equiv p^{e-f} G_e \pmod{p^e}$.
(ii) $p^{e-f} H_f \equiv p^{e-f} H_e \pmod{p^e}$.

Proof. Let $\mathbf{x}_i$ be the row vectors of G_f and $\mathbf{y}_i$ be the row vectors of G_e. Since $G_f = \Psi_f(G_e)$, we have $\mathbf{x}_i \equiv \mathbf{y}_i \pmod{p^f}$. Thus $p^{e-f}\mathbf{x}_i \equiv p^{e-f}\mathbf{y}_i \pmod{p^e}$. This proves (i). The second statement is proved similarly. □

Lemma 2.4. *Let $f < e < \infty$.*

(i) $p^{e-f}\mathscr{C}^f \subset \mathscr{C}^e$.
(ii) $\mathbf{v} = p^f \mathbf{v}_0 \in \mathscr{C}^e$ *iff* $\mathbf{v}_0 \in \mathscr{C}^{e-f}$. *Here, we are assuming that all components of* $\mathbf{v}_0$ *are taken in* $\mathbb{Z}_{p^{e-f}}$.
(iii) $\ker \Psi_f^e = p^f \mathscr{C}^{e-f}$.

Proof. (i) If $\mathbf{v} \in \mathscr{C}^f$, then $H_e(p^{e-f}\mathbf{v})^{\mathrm{T}} \equiv p^{e-f} H_e \mathbf{v}^{\mathrm{T}} \equiv p^{e-f} H_f \mathbf{v}^{\mathrm{T}} \equiv \mathbf{0} \pmod{p^e}$.

(ii) We have $p^f \mathbf{v}_0 \in \mathscr{C}^e \iff p^f H_e(\mathbf{v}_0)^{\mathrm{T}} \equiv 0 \pmod{p^n} \iff p^f H_{e-f}\mathbf{v}_0^{\mathrm{T}} \equiv 0 \pmod{p^n} \iff H_{e-f}\mathbf{v}_0^{\mathrm{T}} \equiv 0 \pmod{p^{e-f}} \iff \mathbf{v}_0 \in \mathscr{C}^{e-f}$.

(iii) $\mathbf{v} \in \ker \Psi_f^e$ if and only if $\mathbf{v} \in \mathscr{C}^e$ and $\mathbf{v} = p^f \mathbf{v}_0$. Thus it follows from (ii). □

The third statement shows that the Hamming weight enumerator of the $\ker \Psi_f^e$ is equal to the Hamming weight enumerator of $\mathscr{C}^{e-f}$.

We now study weights of codewords in lifts of a code. Suppose $f < e$. By Lemma 2.4(i), any weight of a codeword in $\mathscr{C}^f$ is a weight of a codeword in $\mathscr{C}^e$. In other words, if $\mathbf{v} \in \mathscr{C}^f$, then there exists a $\mathbf{w} \in \mathscr{C}^e$ such that $\mathrm{wt}(\mathbf{w}) = \mathrm{wt}(\mathbf{v})$. But the converse is not true in general, as we can see in the next section. Neither is it true that a p-adic code $\mathscr{C}$ must have a codeword of a given weight in $\mathscr{C}^e$. In fact there are examples later in this paper of p-adic codes whose minimum weight is larger than the minimum weight in $\mathscr{C}^e$. However, we do have the following theorem.

Theorem 2.5. *For a p-adic code $\mathscr{C}$*

(i) *the minimum distance $d(\mathscr{C}^e)$ of $\mathscr{C}^e$ is equal to $d = d(\mathscr{C}^1)$ for all $e < \infty$.*
(ii) *the minimum distance $d_\infty = d(\mathscr{C})$ of $\mathscr{C}$ is at least $d(\mathscr{C}^1)$.*

Proof. (i) Let $\mathbf{v}_0$ be a vector in $\mathscr{C}^1$ of weight d. By Lemma 2.4(iii), $p^{e-1}\mathbf{v}_0$ is a codeword of $\mathscr{C}^e$ of weight d. Thus $d(\mathscr{C}^e) \leqslant d$ for all e. We use induction on e and assume that $d(\mathscr{C}^j) = d(\mathscr{C}^1)$ for all $j \leqslant e$. Suppose, on the contrary, that $d(\mathscr{C}^{e+1}) < d$ and let $\mathrm{wt}(\mathbf{v}) < d$ for some nonzero $\mathbf{v} \in \mathscr{C}^{e+1}$. Then $\mathrm{wt}(\Psi_e(\mathbf{v})) \leqslant \mathrm{wt}(\mathbf{v}) < d$. Since $d(\mathscr{C}^e) = d$, we must have $\Psi_e(\mathbf{v}) = \mathbf{0}$ in $\mathscr{C}^e$. This means that $\mathbf{v} = p^e\mathbf{v}_0$. By Lemma 2.4(iii), we have that $\mathbf{0} \neq \mathbf{v}_0 \in \mathscr{C}^1$. Then $0 < w(\mathbf{v}_0) = w(\mathbf{v}) < d$, which is a contradiction.

(ii) Suppose there exists a nonzero codeword $\mathbf{v} \in \mathscr{C}$ with $\mathrm{wt}(\mathbf{v}) < d$. For a sufficiently large N, $\Psi_N(\mathbf{v}) \neq \mathbf{0}$. Then we would have $0 < w(\Psi_N(\mathbf{v})) \leqslant w(\mathbf{v}) < d$, a contradiction. □

Now we discuss the number of codewords of minimum weight. First we need a few lemmas.

Lemma 2.6. *Let k and n be any positive integers and let M be a $k \times n$ matrix over $\mathbb{Z}_{p^e}$ whose standard form has type* $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}0^{k_e}$. *Then* $\ker M = \{\mathbf{x} \in \mathbb{Z}_{p^e}^n \mid M\mathbf{x}^{\mathrm{T}} = \mathbf{0}\}$ *has cardinality*

$$|\ker M| = (1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}(p^e)^{k_e}. \tag{8}$$

Proof. Since the operations (R1), (R2), (R3) do not change the kernel and the operation (C1) only changes the coordinate positions of the vectors in the kernel, we may assume that M is in a standard form as in (4). We have that $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_e) \in \mathbb{Z}_{p^e}^n$, where $\mathbf{x}_i \in \mathbb{Z}_{p^e}^{k_i}$, is in $\ker M$ iff $M\mathbf{x}^{\mathrm{T}} = \mathbf{0}$, i.e.

$$I_{k_0}\mathbf{x}_0^{\mathrm{T}} + A_{01}\mathbf{x}_1^{\mathrm{T}} + \cdots + A_{0,e-1}\mathbf{x}_{e-1}^{\mathrm{T}} + A_{0e}\mathbf{x}_e^{\mathrm{T}} \equiv 0 \pmod{p^e} \tag{9}$$

$$I_{k_1}\mathbf{x}_1^{\mathrm{T}} + \cdots + A_{1,e-1}\mathbf{x}_{e-1}^{\mathrm{T}} + A_{1e}\mathbf{x}_e^{\mathrm{T}} \equiv 0 \pmod{p^{e-1}} \tag{10}$$

$$\cdots \tag{11}$$

$$I_{k_{e-2}}\mathbf{x}_{e-2}^{\mathrm{T}} + A_{e-2,e-1}\mathbf{x}_{e-1}^{\mathrm{T}} + A_{e-2,e}\mathbf{x}_e^{\mathrm{T}} \equiv 0 \pmod{p^2} \tag{12}$$

$$I_{k_{e-1}}\mathbf{x}_{e-1}^{\mathrm{T}} + A_{e-1,e}\mathbf{x}_e^{\mathrm{T}} \equiv 0 \pmod{p}. \tag{13}$$

From these equations, we can see that $\mathbf{x}_e \in \mathbb{Z}_{p^e}^{k_e}$ can be set to be an arbitrary vector, and then (13) determines $\mathbf{x}_{e-1} \pmod{p}$ in a unique way, and then (12) determines $\mathbf{x}_{e-2} \pmod{p^2}$ in a unique way, and so on. Therefore, $|\ker M| = (p^e)^{k_e} \times (p^{e-1})^{k_{e-1}} \times \cdots \times (p^1)^{k_1} \times (1)^{k_0}$. □

Note that $|\ker M|$ is the product of diagonal entries in the standard form, regarding 0's, if any, as p^e.

If $S = \{i_1, \ldots, i_s\}$ is a subset of $\{1, 2, \ldots, n\}$ and $\mathbf{x}$ is a vector of length n, then $\mathbf{x}_S$ denotes the vector of length s obtained from $\mathbf{x}$ by puncturing components outside S. For a given S as above and a vector $\mathbf{y} = (y_1, \ldots, y_k)$ of length s, $\mathbf{y}^S \in \mathbb{Z}_{p^e}^n$ denotes the vector obtained by adjoining 0's outside S, i.e., $\mathbf{y}^S = (x_1, x_2, \ldots, x_n)$ where $x_i = 0$ if $i \notin S$, and $x_{i_j} = y_j$ if $i_j \in S$.

Let $H = (\mathbf{h}_i)$ be the parity check matrix of an $[n, k]$-code C, where $\mathbf{h}_i$ denotes the ith column of H. Let $H_S = (\mathbf{h}_i)_{i \in S}$ be the matrix whose columns are the ith columns of H for $i \in S$. The following is clear from the definition of parity check matrix.

Lemma 2.7. *If* $\mathbf{x} = (x_j)$ *is a codeword of weight* s, *then* $H_S(\mathbf{x}_S)^{\mathrm{T}} = \sum_{j \in S} x_j \mathbf{h}_j = 0$ *where* $S = \mathrm{supp}(\mathbf{x})$ *is the support of* $\mathbf{x}$. *Conversely*, *if* $H_S \mathbf{y}^{\mathrm{T}} = 0$, *then* $\mathbf{y}^S$ is *a codeword of weight equal to* $\mathrm{wt}(\mathbf{y})$.

Let $\mathscr{C}$ be a p-adic $[n, k]$ code, H its parity check matrix and d be the minimum distance of $\mathscr{C}^1$. For each subset $S \subset \{1, 2, \ldots, n\}$ of d elements, let H'_S be the standard form of H_S. Since any $d-1$ columns of $\Psi_1(H)$ are modular independent over $\mathbb{Z}_p$, any matrix consisting of $d-1$ columns of H has the standard form $\begin{pmatrix} I_{d-1} \\ \mathbf{0} \end{pmatrix}$ by Lemma 2.2. Thus H'_S will have type $1^{d-1}(p^j)^1$ for some $j = -\infty, 0, 1, \ldots$. Here we use the convention that $p^{-\infty} = 0$. If $\mathscr{C}^e$ is an MDR code, i.e., $d = n - k + 1$, then all types will be 1^{d-1}, (see [4] for a description of MDR codes). We may regard this type as the type $1^{d-1}(0)^1$ for our purpose. Let μ_j be the number of subsets S for which H'_S has type $1^{d-1}(p^j)^1$.

Theorem 2.8. *The number* A_d^e *of codewords of weight d in* $\mathscr{C}^e$ *is given as follows*:

$$A_d^e = \left(\mu_{-\infty} + \sum_{j \geqslant e} \mu_j \right) (p^e - 1) + \sum_{j=1}^{e-1} \mu_j (p^j - 1). \tag{14}$$

Proof. Let C_d be the set of all codewords of weight d in $\mathscr{C}^e$, and

$$C_S = \{\mathbf{y}^S | \mathbf{0} \neq \mathbf{y} \in \ker(H_e)_S\}$$

for the subsets S of d elements. Clearly $(\mathbf{x}_S)^S = \mathbf{x}$ for any codeword $\mathbf{x}$, where $S = \mathrm{supp}(\mathbf{x})$. Thus C_d is a subset of $\bigcup_S C_S$. Since $\mathrm{wt}(\mathbf{y}^S) = \mathrm{wt}(\mathbf{y})$ and d is the minimum distance of $\mathscr{C}^e$, we have $\mathrm{wt}(\mathbf{y}) = \mathrm{wt}(\mathbf{y}^S) = d$ whenever $\mathbf{0} \neq \mathbf{y} \in \ker(H_e)_S$. Thus $C_d = \bigcup_S C_S$. Furthermore, if $\mathrm{wt}(\mathbf{y}_1) = \mathrm{wt}(\mathbf{y}_2) = d$, then it is clear that $\mathbf{y}_1^{S_1} = \mathbf{y}_2^{S_2}$ iff $\mathbf{y}_1 = \mathbf{y}_2$ and $S_1 = S_2$. Therefore $\bigcup_S C_S$ is a disjoint union and $|C_S| = |\ker(H_e)_S|$.

If H_S has type $1^{d-1}(p^j)^1$ with $1 \leqslant j \leqslant e-1$ then $|\ker(H_e)_S| = p^j$ by Lemma 2.6. On the other hand, if H_S has type $1^{d-1}(p^j)^1$ with $j = \infty$ or $j \geqslant e$, then $(H_e)_S$ has type $1^{d-1}0^1$ and $|\ker(H_e)_S| = p^e$. The theorem is proved. □

Let N be the maximum of $\{j | \mu_j \neq 0\}$.

Corollary 2.9. *For* $e > N$, $A_d^e = ap^e + b$, *where* a, b *are independent of* e. *In other words*, A_d^e *is a linear polynomial in* $q = p^e$, *independent of* e.

Proof. Simply let $a = \mu_{-\infty}$ and $b = \sum_{j=1}^{N} \mu_j (p^j - 1) - \mu_{-\infty}$. □

It is easy to check that

$$A_d^{e+1} - A_d^e = (p^{e+1} - p^e) \left(\mu_{-\infty} + \sum_{j \geqslant e+1} \mu_j \right). \tag{15}$$

From this equation, we obtain the following corollaries.

Corollary 2.10. *If $A_d^1 = A_d^2$, then $A_d^e = A_d^1$ for all e.*

Proof. From (15), we have

$$0 = A_d^2 - A_d^1 = (p^2 - p)\left(\mu_{-\infty} + \sum_{j\geqslant 2} \mu_j\right).$$

Thus $\mu_{-\infty} = 0$ and $\mu_j = 0$ for all $j \geqslant 2$. Hence Eq. (14) reduces to $A_d^e = \mu_1(p-1) = A_d^1$ for all $e \geqslant 2$. □

Corollary 2.11. *Suppose $\mu_{-\infty} = 0$. Then $A_d^e = A_d^N$ for all $e \geqslant N$. In particular, every codeword of weight d in $\mathscr{C}^e$ is of the form $p^{e-N}\mathbf{v}_0$ for some codeword $\mathbf{v}_0$ of weight d in $\mathscr{C}^N$.*

Theorem 2.12. *$\mu_{-\infty} = 0$ if and only if $d_\infty > d$.*

Proof. Recall that $\mathbb{Z}_{p^\infty}$ is an integral domain. Thus if $|S| = d$ and H_S has type $(1)^{d-1}p^j$ with $j \geqslant 0$, then $\ker H_S = \{\mathbf{0}\}$. The theorem follows from Lemma 2.7. □

We generalize our observation to larger weights. Let $\mathscr{C}$ be a p-adic $[n, k]$ code and A_i^e be the number of codewords of weight i in $\mathscr{C}^e$. Then

$$W_{\mathscr{C}^e}(x, y) = \sum_{i=0}^{n} A_i^e x^{n-i} y^i$$

is the weight enumerator of $\mathscr{C}^e$.

Theorem 2.13. *There exist an integer N such that for every $d \leqslant j < d_\infty$, $A_j^e = A_j^N$ for all $e \geqslant N$. In fact, every codeword of weight j in $\mathscr{C}^e$ is of the form $2^{e-N}\mathbf{v}_0$ for some codeword $\mathbf{v}_0$ of weight j in $\mathscr{C}^N$.*

Proof. Let H be the parity check matrix of $\mathscr{C}$ and let K_j be the set of integers m, including $-\infty$, such that p^m appears in the type of H_S for some subset S with $|S| = j$. Take $N = 1 + \max \bigcup_{j=d}^{d_\infty - 1} K_j$. Also, let B_j^e be the number of codewords in $\mathscr{C}^e$ of weight $\leqslant j$.

Suppose $d \leqslant j < d_\infty$ and $e \geqslant N$. Then $-\infty \notin K_j$ for any j and $p^m \not\equiv 0 \pmod{p^e}$ for any integer $m \in K_j$. Therefore, $(H_e)_S = (H_N)_S$ for all S. Thus $|\ker(H_e)_S|$, being a product of diagonal entries of $\Psi_e(H_S')$, is equal to $|\ker(H_N)_S|$. On the other hand, if $\mathbf{y} \in \ker(H_N)_S$, then $p^{e-N}\mathbf{y} \in \ker(H_e)_S$. This implies that $\ker(H_e)_S = 2^{e-N}\ker(H_N)_S$. By Lemma 2.7

$$B_j^e = \left|\bigcup_{|S|=j} \{\mathbf{y}^S | \mathbf{y} \in \ker(H_e)_S\}\right| = \left|\bigcup_{|S|=j} \{2^{e-N}\mathbf{y}^S | \mathbf{y} \in \ker(H_N)_S\}\right| = B_j^N.$$

Therefore $A_j^e = B_j^e - B_{j-1}^e = B_j^N - B_{j-1}^N = A_j^N$. □

3. Examples

In this section, we show some examples and determine their weight enumerators. First we recall the MacWilliams Identity for codes over $\mathbb{Z}_q$, where $q = p^e$.

Theorem 3.1. *Let C be a linear code over $\mathbb{Z}_q$. Then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

The following generalization of Gleason's theorem is essentially proved in [8,10].

Theorem 3.2. *Suppose C is a self-dual code over $\mathbb{Z}_q$ of even length. Then $W_C(x, y)$ is a polynomial in $x^2 + (q-1)y^2$ and $xy - y^2$.*

Example 3.3 (*The 2-adic Hamming code of length 8*). As in [1], we have the 2-adic factorization of

$$x^7 - 1 = (x-1)(x^3 - ax^2 + (a-1)x - 1)(x^3 - (a-1)x - ax - 1),$$

where $a = 0 + 2 + 4 + \cdots$ is a 2-adic number satisfying $a^2 - a + 2 = 0$. By appending 1 to the generator matrix of 2-adic cyclic [7, 4] code with the generator polynomial $x^3 + ax^2 + (a-1)x - 1$, we obtain a 2-adic self-dual [8, 4, 5] code $\mathscr{H}$. In other words, $\mathscr{H}$ has generator matrix

$$G = \begin{pmatrix} -1 & a-1 & a & 1 & 0 & 0 & 0 & 1 \\ 0 & -1 & a-1 & a & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & a-1 & a & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 & a-1 & a & 1 & 1 \end{pmatrix}.$$

Even though $\mathscr{H}$ has minimum distance 5, $\mathscr{H}^1$ and hence all finite lifts $\mathscr{H}^e$ have minimum distance 4. As before, let $W_{\mathscr{H}^e}(x, y) = \sum_{i=0}^{n} A_i^e x^{n-i} y^i$ denote the weight enumerator for $\mathscr{H}^e$. We already know that

$$W_{\mathscr{H}^1}(x, y) = x^8 + 14x^4y^4 + y^8.$$

A calculation by a computer shows that

$$W_{\mathscr{H}^2}(x, y) = x^8 + 14x^4y^4 + 112x^3y^5 + 112xy^7 + 17y^8.$$

Thus $A_4^e = 14$ for all e by Corollary 2.10. By Theorem 3.2,

$$W_{\mathscr{H}^e}(x, y) = \sum_{j=0}^{4} c_i (x^2 + (q-1)y^2)^j (xy - y^2)^{4-j}.$$

Now the identities $A_0^e=1$, $A_1^e=A_2^e=A_3^e=0$ and $A_4^e=14$ completely determine $W^e(x,y)=\sum_{i=0}^{8} A_i^e x^{8-i} y^i$ as follows with $q=2^e$.

$$A_5^e = 56(-2+q),$$
$$A_6^e = 28(8-6q+q^2),$$
$$A_7^e = 8(-22+21q-7q^2+q^3),$$
$$A_8^e = 49-56q+28q^2-8q^3+q^4.$$

Example 3.4 (*3-adic Golay code of length 12*). The 3-adic Golay code $\mathscr{T}$ of length 12 is obtained by adjoining 1 to the generator matrix

$$G=\begin{bmatrix} -1 & a-1 & 1 & -1 & a & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & -1 & a-1 & 1 & -1 & a & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & -1 & a-1 & 1 & -1 & a & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1 & a-1 & 1 & -1 & a & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & -1 & a-1 & 1 & -1 & a & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & -1 & a-1 & 1 & -1 & a & 1 \end{bmatrix}$$

of the 3-adic Golay code of length 11, where we take $a \equiv 0 \pmod 3$ to be the 3-adic solution of the equation $a^2-a+3=0$. $\mathscr{T}$ is a 3-adic lift of the extended ternary [12, 6, 6] Golay code. $\mathscr{T}$ has minimum distance 7, while all finite $\mathscr{T}^e$ have minimum distance 6. It is well-known that

$$W_{\mathscr{T}^1}(x,y)=x^{12}+264x^6y^6+440x^3y^9+24y^{12}.$$

One can check that $A_6^2=264$. Therefore, $A_6^e=264$ for all e as well. As before,

$$W_{\mathscr{T}^e}(x,y)=\sum_{j=0}^{6} c_j(x^2+(q-1)y^2)^j(xy-y^2)^{6-j}.$$

Again, $A_0^e=1$, $A_1^e=A_2^e=A_3^e=A_4^e=A_3^5=0$ and $A_6^e=264$ determine A_i^e as follows, with $q=3^e$.

$$A_7^e = 792(-3+q),$$
$$A_8^e = 495(15-8q+q^2),$$
$$A_9^e = 220(-52+36q-9q^2+q^3),$$
$$A_{10}^e = 66(144-120q+45q^2-10q^3+q^4),$$
$$A_{11}^e = 12(-342+330q-165q^2+55q^3-11q^4+q^5),$$
$$A_{12}^e = 726-792q+495q^2-220q^3+66q^4-12q^5+q^6.$$

This weight enumerator was first computed in [7].

Example 3.5 (*Yet another lift of the ternary Golay code*). There exists a very simple 3-adic self-dual lift $\mathscr{P}$ of the ternary Golay code [3]. The code $\mathscr{P}$ is defined by the generator matrix

$$G = \left(I_6 \left| \begin{matrix} 0 & b & b & b & b & b \\ b & 0 & b & -b & -b & b \\ b & b & 0 & b & -b & -b \\ b & -b & b & 0 & b & -b \\ b & -b & -b & b & 0 & b \\ b & b & -b & -b & b & 0 \end{matrix} \right. \right), \tag{16}$$

where b is a 3-adic number satisfying $5b^2+1=0$ with $\Psi_1(b)=2$. $\mathscr{P}$ has minimum distance 6, in contrast to $d(\mathscr{T})=7$. One can check that

$$\mu_{-\infty}=72, \quad \mu_1=60, \quad \mu_j=0 \quad \text{for all } j \geqslant 2$$

by computing the determinants of all possible 6×6 submatrices of G. By Theorem 2.8,

$$A_6^e = 72(q-1)+60(3-1)=24(2+3q).$$

As before, we then get the weight enumerators of $\mathscr{P}^e$ as follows, with $q=3^e$.

$$A_6^e = 24(2+3q),$$
$$A_7^e = 360(-3+q),$$
$$A_8^e = 45(93-64q+11q^2),$$
$$A_9^e = 20(-356+324q-99q^2+11q^3),$$
$$A_{10}^e = 6(1044-1140q+495q^2-110q^3+11q^4),$$
$$A_{11}^e = 12(-234+294q-165q^2+55q^3-11q^4+q^5),$$
$$A_{12}^e = 510-720q+495q^2-220q^3+66q^4-12q^5+q^6.$$

Example 3.6 (*2-adic Golay code of length 24*). The binary Golay code is lifted to a 2-adic code using the cyclic generator

$$\begin{aligned}\pi(x) = x^{11} &+ ax^{10} + (a-3)x^9 - 4x^8 - (a+3)x^7 - (2a+1)x^6 \\ &- (2a-3)x^5 - (a-4)x^4 + 4x^3 + (a+2)x^2 + (a-1)x - 1,\end{aligned}$$

where a is a 2-adic number satisfying $a^2-a+6=0$ with $\Psi_2(a)=0$. We extend this code by appending 1 to the generators and obtain a self-dual 2-adic [24,12,13] code $\mathscr{G}$ [1]. Note that all finite $\mathscr{G}^e$ are [24, 12, 8] codes. It is much harder to find the weight enumerators than before, since all finite $\mathscr{G}^e$ have more unknowns in their weight enumerators. The weight enumerator of the binary Golay codes is known to be

$$W_{\mathscr{G}^1}(x,y) = x^{24}+759x^{16}y^8+2576x^{12}y^{12}+759x^8y^{16}+y^{24}.$$

One can compute

$$\begin{aligned}W_{\mathscr{G}^2} = {} & x^{24} + 759x^{16}y^{8} + 12144x^{14}y^{10} + 172592x^{12}y^{12} + 61824x^{11}y^{13} \\ & + 765072x^{10}y^{14} + 1133440x^{9}y^{15} + 1239447x^{8}y^{16} + 4080384x^{7}y^{17} \\ & + 1445136x^{6}y^{18} + 4080384x^{5}y^{19} + 1870176x^{4}y^{20} + 1133440x^{3}y^{21} \\ & + 692208x^{2}y^{22} + 61824xy^{23} + 28385y^{24}\end{aligned}$$

and find $A_8^2 = 759 = A_8^1$. Therefore, $A_8^e = 759$ for all e. Note that $A_9^1 = A_9^2 = 0$.

Theorem 3.7. *$A_9^e = 0$ for all e.*

Proof. If not, there exists an integer $e \geqslant 3$ such that $A_9^{e+1} \neq 0$, $A_9^e = 0$. Take a codeword $\mathbf{x} \in \mathscr{G}^{e+1}$ of weight 9. If all components of $\mathbf{x}$ is even, then $\mathbf{x} = 2\mathbf{x}_0$, which implies that $\mathbf{x}_0 \in \mathscr{G}^e$ is a codeword of weight 9, a contradiction. Therefore some component of $\mathbf{x}$ is odd. Then $\Psi_j(\mathbf{x}) \neq \mathbf{0}$. In particular, $\Psi_2(\mathbf{x})$ is a codeword of $\mathscr{G}^2$ of weight 8. But since $A_8^2 = A_8^1$, we know that all codewords in $\mathscr{G}^2$ of weight 8 have the form $2\mathbf{x}_0$ for some $\mathbf{x}_0 \in \mathscr{G}^1$. This leads to another contradiction. □

Now

$$W_{\mathscr{G}^e}(x) = \sum_{j=0}^{12} c_j (x^2 + (q-1)y^2)^j (xy - y^2)^{12-j}.$$

Since we know A_0^e to A_9^e for each e, there are three unknown to be determined. But Theorem 2.13 tells us that A_{10}^e, A_{11}^e, A_{12}^e remain constant for $e \geqslant N$, where N is given in the proof of the theorem. A computer calculation shows that $N = 7$. This means that once we know $W_{\mathscr{G}^e}(x, y)$ for $e = 3, 4, 5, 6, 7$, then we know all weight enumerators of lifts of the Golay code. The A_j^e are then easily computed. They can be found at [2].

Acknowledgements

Young Ho Park would like to thank Steven Dougherty and the Mathematics Department of the University of Scranton for their hospitality while he finished this work during his sabbatical stay.

References

[1] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Designs Codes Cryptogr. 6 (1995) 21–35.
[2] S.T. Dougherty, Computation of the A_j^e for the Golay code, <http://academic.scranton.edu/faculty/doughertys1/golay.htm>.
[3] S.T. Dougherty, Y.H. Park, Codes over the p-adic integers, Designs, Codes Cryptogr., 2004, in preparation.
[4] S.T. Dougherty, K. Shiromoto, MDR codes over Z_k, IEEE Trans. Inform. Theory 46 (1) (2000) 265–269.

[5] I.M. Duursma, M. Greferath, Computing symmetrized weight enumerators for lifted quadratic residue codes, preprint, 2003, <http://adsabs.harvard.edu/preprint_service.html>.
[7] S.Y. Kim, Liftings of the ternary Golay code, Master's Thesis, Kangwon National University, 2004.
[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, Amsterdam, 1977.
[9] G.H. Norton, Ana Salagean, On the Hamming distance of linear codes over a finite chain ring, IEEE Trans. Inform. Theory 46 (2000) 1060–1067.
[10] E. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), The Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 177–294.
[11] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121 (3) (1999) 555–575.