Bull. Korean Math. Soc. **54** (2017), No. 3, pp. 731–736
https://doi.org/10.4134/BKMS.b151011
pISSN: 1015-8634 / eISSN: 2234-3016

A CONSTRUCTION OF TWO-WEIGHT CODES AND ITS APPLICATIONS

Eun Ju Cheon, Yuuki Kageyama, Seon Jeong Kim, Namyong Lee, and Tatsuya Maruta

Abstract. It is well-known that there exists a constant-weight $[s\theta_{k-1}, k, sq^{k-1}]_q$ code for any positive integer s, which is an s-fold simplex code, where $\theta_j = (q^{j+1}-1)/(q-1)$. This gives an upper bound $n_q(k, sq^{k-1}+d) \leq s\theta_{k-1} + n_q(k, d)$ for any positive integer d, where $n_q(k, d)$ is the minimum length n for which an $[n, k, d]_q$ code exists. We construct a two-weight $[s\theta_{k-1}+1, k, sq^{k-1}]_q$ code for $1 \leq s \leq k-3$, which gives a better upper bound $n_q(k, sq^{k-1}+d) \leq s\theta_{k-1} + 1 + n_q(k-1, d)$ for $1 \leq d \leq q^s$. As another application, we prove that $n_q(5, d) = \sum_{i=0}^{4} \lceil d/q^i \rceil$ for $q^4 + 1 \leq d \leq q^4 + q$ for any prime power q.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q. For a nonzero vector $x \in \mathbb{F}_q^n$, the weight of x, denoted by $wt(x)$, is the number of nonzero positions in x. An $[n, k, d]_q$ code C is a k-dimensional linear subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$ with minimum (Hamming) weight d, where $d = \min\{wt(x) \mid x \in C, x \neq \mathbf{0}\}$. For an $[n, k, d]_q$ code C, let A_i be the number of codewords in C of weight i. The weight enumerator of C is defined as a polynomial $W_C(z) = \sum_{i=0}^{n} A_i z^i$, where z is an indeterminate.

The optimal linear code problem is to optimize one of the parameters n, k and d when the other two are given ([3]). In particular, we consider the problem to find $n_q(k, d)$, the minimum length n for which an $[n, k, d]_q$ code exists. For an $[n, k, d]_q$ code, there is an important lower bound on the length n which is called the Griesmer bound. The Griesmer bound, proved by Griesmer [2] for

Received December 9, 2015.
2010 *Mathematics Subject Classification.* 94B27, 94B05, 51E20, 05B25.
Key words and phrases. linear code, two-weight code, length optimal code, Griesmer bound, projective space.
The first author was supported by the National Research Foundation of Korea funded by the Korean Government(NRF-2014R1A1A3053319).
The third author was partially supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2042228).
The last author was partially supported by JSPS KAKENHI Grant Number JP16K05256.

binary case and Solomon and Stiffler [10] for arbitrary q, gives the following:

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. A code meeting the Griesmer bound is called *Griesmer*. The values of $n_q(k,d)$ are determined for all d only for some small values of q and k, see [9]. We note that for $k = 1, 2$, there are Griesmer codes for all d and hence $n_q(k,d) = g_q(k,d)$. So, we only consider $k \geq 3$.

An important class of Griesmer codes are s-fold simplex codes, which are constant-weight $[s\theta_{k-1}, k, sq^{k-1}]_q$ codes with a positive integer s, where $\theta_j = (q^{j+1}-1)/(q-1) = q^j + q^{j-1} + \cdots + q + 1$. It is well-known that a large class of Griesmer codes which are called codes of Belov type can be constructed from s-fold simplex codes by puncturing if the condition in the following theorem is satisfied. Belov *et al.* [8] proved the theorem for $q = 2$ and Hill [3] generalized it to arbitrary q.

Theorem 1.1 ([3, Theorem 2.12], [8])**.** *Let $d = sq^{k-1} - \sum_{i=1}^{p} q^{u_i - 1}$ such that $k > u_1 \geq u_2 \geq \cdots \geq u_p$ with $u_i > u_{i+q-1}$ for $1 \leq i \leq p-q+1$, where $s = \lceil \frac{d}{q^{k-1}} \rceil$. Then there exists a $[g_q(k,d), k, d]_q$ code of Belov type if and only if $\sum_{i=1}^{\min\{s+1,p\}} u_i \leq sk$.*

On the other hand, many optimal codes can be constructed from s-fold simplex codes by extension. The following lemmas are often used to extend codes from known codes.

Lemma 1.2 ([5])**.** *Let C be an $[n,k,d]_q$ code and C' an $[n',k,d']_q$ code. Then there exists an $[n+n', k, d+d']_q$ code.*

Lemma 1.3 ([5])**.** *Let C be an $[n,k-1,d]_q$ code and C' an $[n',k,d']_q$ code. If there is a codeword $\mathbf{c} \in C'$ with $wt(\mathbf{c}) \geq d+d'$, then there exists an $[n+n', k, d+d']_q$ code.*

One can apply Lemma 1.2 to get the following when the code C' is an $[s\theta_{k-1}, k, sq^{k-1}]_q$ code, but cannot apply Lemma 1.3 since C' is constant-weight.

Corollary 1.4. *$n_q(k, sq^{k-1}+d) \leq s\theta_{k-1} + n_q(k,d)$ for any positive integer d.*

Especially when $n_q(k,d) = g_q(k,d)$, the extended code is also Griesmer.

Corollary 1.5. *$n_q(k, sq^{k-1}+d) = g_q(k, sq^{k-1}+d)$ if $n_q(k,d) = g_q(k,d)$.*

For example, we have $n_5(5,627) = g_5(5,627)$ from $n_5(5,2) = g_5(5,2)$. But when $n_q(k,d) > g_q(k,d)$, Corollary 1.4 does not always give a good upper bound on $n_q(k, sq^{k-1}+d)$. In this paper, we construct a new class of two-weight $[s\theta_{k-1}+1, k, sq^{k-1}]_q$ codes for $1 \leq s \leq k-3$, which give a better upper bound on $n_q(k, sq^{k-1}+d)$. See [1] for two-weight linear codes and related combinatorial objects. Our main result is the following.

Theorem 1.6. *For two integers k and s with $1 \le s \le k-3$, there exists a two-weight $[s\theta_{k-1}+1, k, sq^{k-1}]_q$ code with weight enumerator*

$$W_C(z) = 1 + (q^k - q^{k-s} + q^{k-s-1} - 1)z^{sq^{k-1}} + (q^{k-s} - q^{k-s-1})z^{sq^{k-1}+q^s}.$$

Theorem 1.6 is a generalization of Lemma 3.2 in [7]. Applying Lemma 1.3 with the $[s\theta_{k-1}+1, k, sq^{k-1}]_q$ code in Theorem 1.6 as C', one can get the following.

Theorem 1.7. *$n_q(k, sq^{k-1}+d) \le s\theta_{k-1}+1+n_q(k-1,d)$ for integers $1 \le s \le k-3$ and $1 \le d \le q^s$.*

Note that Theorem 1.7 is better than Corollary 1.4 since $n_q(k,d) \ge n_q(k-1,d)+1$ [5]. For instance, we have $n_5(5, 1270 = 20+2q^4) \le g_5(5,1270)+2$ by Corollary 1.4, for $n_5(5,20) = g_5(5,20)+1$ or $g_5(5,20)+2$, see [9]. But Theorem 1.7 with $q = k = 5$ and $s = 2$ and the Griesmer bound yield that $n_5(5,1270) = g_5(5,1270)$ since $n_5(4,20) = g_5(4,20)$. Thus one can get Griesmer codes when $n_q(k-1,d) = g_q(k-1,d)$ by Theorem 1.7 as follows.

Corollary 1.8. *Let k, d and s be integers with $1 \le s \le k-3$ and $1 \le d \le q^s$. Then $n_q(k, sq^{k-1}+d) = g_q(k, sq^{k-1}+d)$ if $n_q(k-1,d) = g_q(k-1,d)$.*

We have more pairs (k,d) for which $n_q(k,d) = g_q(k,d)$ holds.

Theorem 1.9. *For any q, k and r with $1 \le s \le k-3 \le q-1$, we have $n_q(k,d) = g_q(k,d)$ for $sq^{k-1} \le d \le sq^{k-1}+q-k+3$.*

From Theorem 1.1, we have $n_q(k,d) = g_q(k,d)$ for $(k-3)q^{k-1}-(k-3)q^{k-2}-q^{k-3}+1 \le d \le (k-3)q^{k-1}$ if $k \ge 4$. Hence, from Theorem 1.9 with $s = k-3$, we get the following.

Corollary 1.10. *We have $n_q(k,d) = g_q(k,d)$ for $k \ge 4$ and*

$$(k-3)q^{k-1}-(k-3)q^{k-2}-q^{k-3}+1 \le d \le (k-3)q^{k-1}+q-k+3.$$

For $k = 5$, it is known that $n_q(5,d) = g_q(5,d)$ for $q^4-2q^2+1 \le d \le q^4$. As another application of Theorem 1.6, we expand the known range of Griesmer codes as follows.

Theorem 1.11. *For any q, we have $n_q(5,d) = g_q(5,d)$ for $q^4+1 \le d \le q^4+q$.*

2. Proof of main results

For a positive integer r, let $\mathbb{P}^r$ be the r-dimensional projective space over $\mathbb{F}_q$. Let θ_r be the number of points in $\mathbb{P}^r$, that is, $\theta_r := q^r + \cdots + q + 1$. By convention, we let $\theta_0 := 1$ and $\theta_r := 0$ for $r < 0$. We call a projective subspace of dimension j in $\mathbb{P}^r$ a j-flat. In this paper, points, lines, planes, and hyperplanes refer to flats of dimension 0, 1, 2, and $r-1$ in $\mathbb{P}^r$, respectively.

Let C be an $[n,k,d]_q$ code with a generator matrix G. Each column of G can be regarded as a point of $\mathbb{P}^{k-1}$ if every column of G is nonzero. The formal sum of all columns of G as points in $\mathbb{P}^{k-1}$ is called a 0-cycle of the code C, denoted by $\mathcal{X}_C$. Denoting $m(P) \geq 0$ the number of times of the point P occurring as a column of G, we have $\mathcal{X}_C = \sum_{P \in \mathbb{P}^{k-1}} m(P)P$. We define the degree of $\mathcal{X}_C$ as $\deg \mathcal{X}_C = \sum_{P \in \mathbb{P}^{k-1}} m(P)$. For a subset S in $\mathbb{P}^{k-1}$, we denote $[S] := \sum_{P \in S} P$, which can be identified with the set S. We denote $\mathcal{X}_C(S) = \sum_{P \in S} m(P)P$ the restriction of $\mathcal{X}_C$ to S, and $m_C(S) = \deg \mathcal{X}_C(S) = \sum_{P \in S} m(P)$. Then we have the parameters of C as follows;

$$\begin{aligned} n &= \deg \mathcal{X}_C, \\ d &= n - \max\{m_C(H) \mid H \text{ is a hyperplane in } \mathbb{P}^{k-1}\}. \end{aligned}$$

We let

$$C_i = \{P \in \mathbb{P}^{k-1} \mid m(P) = i\} \text{ and } \gamma_j = \max\{m_C(L) \mid L \text{ is an } j\text{-flat in } \mathbb{P}^{k-1}\}.$$

Note that γ_0 is the maximum multiplicity of points in $\mathbb{P}^{k-1}$ and we have the partition $\mathbb{P}^{k-1} = \cup_{i=0}^{\gamma_0} C_i$. When $\mathbb{P}^{k-1} = C_s$ with positive integer s, C is a Griesmer $[s\theta_{k-1}, k, sq^{k-1}]_q$ code, which is called an *s-fold simplex code*.

There are some interesting Griesmer codes not of Belov type, which are constructed from geometrical objects in projective geometry. Recall that a t-arc in $\mathbb{P}^{k-1}$ means the set of t points, no k points of them are contained in a hyperplane in $\mathbb{P}^{k-1}$ ([6]).

Example 2.1. (1) Let C be a linear code of $\mathcal{X}_C = [\mathcal{C}]$, where $\mathcal{C}$ is a conic in $\mathbb{P}^2$. Then the code C is a $[q+1, 3, q-1]_q$ Griesmer code. In general, a normal rational curve is a $(q+1)$-arc in $\mathbb{P}^{k-1}$, which corresponds to a $[q+1, k, q-k+2]_q$ Griesmer code for $q > k-2$.

(2) Let C be a linear code of $\mathcal{X}_C = [\mathcal{O}]$, where $\mathcal{O}$ is an ovoid in $\mathbb{P}^3$. Then the code C is a $[q^2+1, 4, q^2-q]_q$ Griesmer code.

Proof of Theorem 1.6. For two integers k and r with $2 \leq r \leq k-2$, consider an r-flat Δ in $\mathbb{P}^{k-1}$ and q $(r-1)$-flats $L_1, \ldots, L_q$ in Δ satisfying that no $r+1$ of $\{L_1, \ldots, L_q\}$ are concurrent. Let C be a code with $\mathcal{X}_C = (r-1)[\mathbb{P}^{k-1}] + [\Delta] - \sum_{i=1}^{q}[L_i]$. We shall show that C is an $[(r-1)\theta_{k-1}+1, k, (r-1)q^{k-1}]_q$ code. More precisely, C is a two-weight code with the weight enumerator

$$W_C(z) = 1 + (q^k - q^{k-r+1} + q^{k-r} - 1)z^{(r-1)q^{k-1}} + (q^{k-r+1} - q^{k-r})z^{(r-1)q^{k-1}+q^{r-1}}.$$

Note that $n = (r-1)\theta_{k-1} + \theta_r - q\theta_{r-1} = (r-1)\theta_{k-1} + 1$. Let H be a hyperplane in $\mathbb{P}^{k-1}$.

If H contains Δ, then we have $\mathcal{X}_C(H) = (r-1)[H] + [\Delta] - \sum_{i=1}^{q}[L_i]$, hence $m_C(H) = (r-1)\theta_{k-2} + \theta_r - q\theta_{r-1} = (r-1)\theta_{k-2} + 1$. Thus the weight of the codeword corresponding to H is $(r-1)q^{k-1}$.

If H does not contain Δ, then we have two cases. (i) If H contains one of L_i, say L_1, then we have $\mathcal{X}_C(H) = (r-1)[H] + [L_1] - \sum_{i=1}^{q}[L_i \cap L_1]$, hence $m_C(H) = (r-1)\theta_{k-2} - (q-1)\theta_{r-2}$ and hence we have a weight $(r-1)q^{k-1} + q^{r-1}$. Thus the weight of the codeword corresponding to H is $(r-1)q^{k-1} + q^{r-1}$. (ii) If H does not contain L_i for any $i = 1, \ldots, q$, then we have $\mathcal{X}_C(H) =$

$(r-1)[H]+[\Delta\cap H]-\sum_{i=1}^{q}[L_i\cap H]$, hence $m_C(H)=(r-1)\theta_{k-2}+\theta_{r-1}-q\theta_{r-2}$. Thus the weight of the codeword corresponding to H is $(r-1)q^{k-1}$.

Thus C is a two-weight code. The number of codewords of weight $(r-1)q^{k-1}+q^{r-1}$ is $(q-1)\#\{H \mid H \not\supset \Delta \text{ and } H \supset L_i \text{ for some } i=1,\dots,q\}$ which is $(q-1)q^{k-r}$. Setting $s=r-1$, we obtain Theorem 1.6. □

Proof of Corollary 1.8. Since there exists a $[g_q(k-1,d),k-1,d]_q$ code, by Lemma 1.3 and Theorem 1.6, there exists a $[g_q(k-1,d)+s\theta_{k-1}+1,k,d+sq^{k-1}]_q$ code, say C. Since $d\le q^s$ we have $g_q(k,d)=g_q(k-1,d)+\lceil\frac{d}{q^{k-1}}\rceil=g_q(k-1,d)+1$. We express d uniquely as the form $d=q^{k-1}-\sum_{i=0}^{k-2}d_iq^i$ with $0\le d_i\le q-1$, $i=0,1,\dots,k-2$. Then $g_q(k,d)=\theta_{k-1}-\sum_{i=0}^{k-2}d_i\theta_i$. Since $d+sq^{k-1}=(s+1)q^{k-1}-\sum_{i=0}^{k-2}d_iq^i$, we have

$$\begin{aligned} g_q(k,d+sq^{k-1}) &= (s+1)\theta_{k-1}-\sum_{i=0}^{k-2}d_i\theta_i \\ &= g_q(k,d)+s\theta_{k-1}=g_q(k-1,d)+1+s\theta_{k-1} \end{aligned}$$

which is just the length of C and we complete the proof. □

Proof of Theorem 1.9. By Example 2.1(1), we have a Griesmer $[q+1,k-1,q-k+3]_q$ code. By Corollary 1.8, we have $n_q(k,q-k+3+sq^{k-1})=g_q(k,q-k+3+sq^{k-1})$. The rest of the codes required for the theorem can be obtained by puncturing. □

Proof of Theorem 1.11. It suffices to construct a $[g_q(5,d),5,d]_q$ code for $d=q^4+q$. From Theorem 1.6 with $k=5$ and $r=2$, one can get a $[\theta_4+1,5,q^4]_q$ code C with non-zero weights q^4 and q^4+q. Take a hyperplane H with $m_C(H)=\theta_3+1-q$ in $\mathbb{P}^4$. Then, $H\cap\Delta=L_j$ for some j with $1\le j\le q$, where the plane Δ and the q lines $L_1,\dots,L_q$ in Δ are taken as in Theorem 1.6. So, we have $\mathcal{X}_C(H)=[H]-\sum_{i\ne j}[L_i\cap L_j]$, and we can take $q-2$ skew lines $m_1,\dots,m_{q-2}$ in H which are skew to L_j. Let C' be a code with 0-cycle $\mathcal{X}_{C'}=\mathcal{X}_C-\sum_{i=1}^{q-2}[m_i]$. Then C' is a $[\theta_4+1-(q-2)\theta_1,5,q^4-q(q-2)]_q$ code containing a codeword of weight q^4+q. Applying Lemma 3 to this C' and a $[q^2+1,4,q^2-q]_q$ code in Example 2.1(2), one can get a Griesmer $[\theta_4+q+4,5,q^4+q]_q$ code. □

References

[1] R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986), no. 2, 97–122.

[2] J. H. Griesmer, *A bound for error-correcting codes*, IBM J. Res. Develop. **4** (1960), 532–542.

[3] R. Hill, *Optimal linear codes*, Cryptography and coding, II (Cirencester, 1989), 75–104, Inst. Math. Appl. Conf. Ser. New Ser., 33, Oxford Univ. Press, New York, 1992.

[4] R. Hill and E. Kolev, *A survey of recent results on optimal linear codes*, Combinatorial Designs and their Applications (Milton Keynes, 1997), 127–152, Chapman Hall/CRC Res. Notes Math., 403, Chapman Hall/CRC, Boca Raton, FL, 1999.

[5] R. Hill and D. E. Newton, *Optimal ternary linear codes*, Des. Codes Cryptogr. **2** (1992), no. 2, 137–157.
[6] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Clarendon Press, Oxford, 1998.
[7] Y. Kageyama and T. Maruta, *On the construction of Griesmer codes of dimension 5*, Des. Codes Cryptogr. **75** (2016), no. 2, 277–280.
[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland: New York, 1977.
[9] T. Maruta, *Griesmer bound for linear codes over finite fields*, http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer/.
[10] G. Solomon and J. J. Stiffler, *Algebraically punctured cyclic codes*, Inform. and Control **8** (1965), no. 2, 170–179.

Eun Ju Cheon
Department of Mathematics and RINS
Gyeongsang National University
Jinju 52828, Korea
E-mail address: enju1000@naver.com

Yuuki Kageyama
Department of Mathematics and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
E-mail address: maruta@mi.s.osakafu-u.ac.jp

Seon Jeong Kim
Department of Mathematics and RINS
Gyeongsang National University
Jinju 52828, Korea
E-mail address: skim@gnu.ac.kr

Namyong Lee
Department of Mathematics and Statistics
Minnesota State University
Mankato, MN 56001, USA
E-mail address: namyong.lee@mnsu.edu

Tatsuya Maruta
Department of Mathematics and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
E-mail address: maruta@mi.s.osakafu-u.ac.jp