AN EXPLICIT FORMULA FOR A WEIGHT ENUMERATOR OF LINEAR-CONGRUENCE CODES

TARO SAKURAI

ABSTRACT. An explicit formula for a weight enumerator of linear-congruence codes is provided. This extends the work of Bibak and Milenkovic [IEEE ISIT (2018) 431–435] addressing the binary case to the non-binary case. Furthermore, the extension simplifies their proof and provides a complete solution to a problem posed by them.

KEYWORDS AND PHRASES. weight enumerator, code size, linear-congruence code, exponential sum

August 29, 2018.
2010 Mathematics Subject Classification: 94B60 (05A15, 11L15)
Source: https://arxiv.org/abs/1808.09365v1

INTRODUCTION

Throughout this article, n and m denote positive integers, b denotes an integer and $\mathbb{Z}_q \coloneqq \{0, 1, \ldots, q-1\} \subset \mathbb{Z}$ for a positive integer q. We will use n for a code length, m for a modulus, b for a defining parameter of a code and $\mathbb{Z}_q$ for a code alphabet.

Definition. Let $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$. The set C of all the solutions $x = (x_1, \ldots, x_n) \in \mathbb{Z}_q^n$ for a linear congruence equation

$$a \cdot x \equiv b \pmod{m} \tag{1}$$

is said to be a *linear-congruence code* where $a \cdot x \coloneqq a_1x_1 + \cdots + a_nx_n$. A linear-congruence code C is called *binary* when $q = 2$.

Several deletion-correcting codes which have been studied are linear-congruence codes; the Varshamov-Tenengol'ts codes , the Levenshtein codes , the Helberg codes , the Le-Nguyen codes , the construction C' of Hagiwara (for some parameters), the consecutively systematic encodable codes and the ternary integer codes in fall into this category (Table).

TABLE. Examples of linear-congruence codes

Linear-congruence code	q	$(a_1, \ldots, a_n)$	m	Constraints
Varshamov-Tenengol'ts code	2	$(1, \ldots, n)$	$n + 1$	
Levenshtein code	2	$(1, \ldots, n)$	m	$m \geq n + 1$
Helberg code	2	$(v_1, \ldots, v_n)$	v_{n+1}	$s \in \mathbb{Z}_{>0}$
Le-Nguyen code	q	$(w_1, \ldots, w_n)$	m	$m \geq w_{n+1}, s \in \mathbb{Z}_{>0}$
Construction C'	2	$(c_1, \ldots, c_n)$	n	$b \not\equiv 0, n(n+1)/2 \pmod{n}$
Consecutively systematic encodable codes	2	$(b_1, \ldots, b_n)$	2^{s+1}	$b = 0, s \in \mathbb{Z}_{>0}, 0 < n - s < 2^{s-1}$
Ternary integer code	3	$(t_1, \ldots, t_n)$	$2^{n+1} - 1$	

The following problem concerning the size of a linear-congruence code—the number of solutions for a linear congruence equation [eq: ax = b]—is posed by Bibak and Milenkovic.

Problem. Give an explicit formula for the size of a linear-congruence code.
Finding an explicit formula would be a first step toward understanding the asymptotic behavior of the size of a linear-congruence code. Bibak and Milenkovic provide a solution to the problem for the binary case. In this article, we provide a complete solution to the problem with a simple proof, which improves the argument of Bibak and Milenkovic. Actually, what we will show is how the Hamming weights of the solutions for a linear congruence equation distribute. This immediately gives an expression of the size of a linear-congruence code involving exponential sums—Weyl sums of degree one.

To state the main theorem we need notation which will be standard.

Definition. For a code $C \subseteq \mathbb{Z}_q{}^n$, we define a polynomial $W_C(z)$ by

$$W_C(z) = \sum_{x \in C} z^{wt(x)} = \sum_{i=0}^{n} A_i(C) z^i,$$

where $wt(x)$ denotes the Hamming weight and

$$A_i(C) \coloneqq |x \in C : wt(x) = i| \qquad (0 \leq i \leq n).$$

The polynomial $W_C(z)$ is said to be the (non-homogeneous) *weight enumerator* of the code C.
Following custom due to Vinogradov in additive number theory, $e(\alpha)$ denotes $e^{2\pi\alpha\sqrt{-1}}$ for $\alpha \in \mathbb{R}$. Now we are in position to state our main theorem.

Theorem. Let $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$. Then the weight enumerator $W_C(z)$ of the linear-congruence code

$$C = x \in \mathbb{Z}_q^n : a \cdot x \equiv b \pmod{m} \tag{2}$$

is given by

$$W_C(z) = \frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\prod_{i=1}^{n}\left(1 + ze\left(\frac{ja_i}{m}\right) + \cdots + ze\left(\frac{ja_i(q-1)}{m}\right)\right). \tag{3}$$

With the same notation as above, the size of the code C is given by

$$|C| = \frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\prod_{i=1}^{n}\left(1 + e\left(\frac{ja_i}{m}\right) + \cdots + e\left(\frac{ja_i(q-1)}{m}\right)\right).$$

PROOF OF THEOREM

The only lemma we need to prove the main theorem is the following trivial one.

$$\frac{1}{m}\sum_{j=1}^{m} e\left(\frac{jb}{m}\right) = \begin{cases} 1 & \text{if } b \equiv 0 \pmod{m} \\ 0 & \text{if } b \not\equiv 0 \pmod{m}. \end{cases}$$

The proof is straightforward:

$$\begin{aligned}
&\frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\prod_{i=1}^{n}\left(1 + ze\left(\frac{ja_i}{m}\right) + \cdots + ze\left(\frac{ja_i(q-1)}{m}\right)\right) \\
&= \frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\prod_{i=1}^{n}\sum_{x_i \in \mathbb{Z}_q} z^{wt(x_i)} e\left(\frac{ja_i x_i}{m}\right) \\
&= \frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\sum_{(x_1,\ldots,x_n)\in\mathbb{Z}_q^n}\prod_{i=1}^{n} z^{wt(x_i)} e\left(\frac{ja_i x_i}{m}\right) \\
&= \frac{1}{m}\sum_{j=1}^{m} e\left(-\frac{jb}{m}\right)\sum_{x\in\mathbb{Z}_q^n} z^{wt(x)} e\left(\frac{ja\cdot x}{m}\right) \\
&= \sum_{x\in\mathbb{Z}_q^n}\left(\frac{1}{m}\sum_{j=1}^{m} e\left(\frac{j(a\cdot x - b)}{m}\right)\right) z^{wt(x)} \\
&= \sum_{x\in C} z^{wt(x)} \qquad \text{(By Lemma.)} \\
&= W_C(z).
\end{aligned}$$

Remark. The original proof by Bibak and Milenkovic for the binary case uses a theorem of Lehmer , which states a linear congruence equation

$$a \cdot x \equiv b \pmod{m}$$

defined by $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$ has a solution $x \in {\mathbb{Z}_m}^n$ if and only if $\gcd(a_1, \ldots, a_n, m)$ divides b. Consequently, their result is stated depending on whether $\gcd(a_1, \ldots, a_n, m)$ divides b or not. By contrast, our result does not refer to $\gcd(a_1, \ldots, a_n, m)$ because our proof does not rely on the Lehmer theorem.

ACKNOWLEDGMENTS

The author thanks Professor Manabu Hagiwara for drawing the author's attention to the work of Bibak and Milenkovic and his invaluable help during the preparation of this article. This work is partially supported by KAKENHI(B) 18H01435, 16K12391 and 16K06336.

REFERENCES

[1] K. Bibak and O. Milenkovic, Weight enumerators of some classes of deletion correcting codes, *IEEE ISIT* (2018) 431–435, doi:10.1109/ISIT.2018.8437121.

[2] M. Hagiwara, On ordered syndromes for multi insertion/deletion error-correcting codes, *IEEE ISIT* (2016) 625–629, doi:10.1109/ISIT.2016.7541374.

[3] Perfect codes for single balanced adjacent deletions, *IEEE ISIT* (2017) 1938–1942, doi:10.1109/ISIT.2017.8006867.

[4] A. S. J. Helberg and H. C. Ferreira, On multiple insertion/deletion correcting codes, *IEEE Trans. Inf. Theory* ***48*** (2002) 305–308, doi:10.1109/18.971760. MR 1872185 Zbl 1059.94040

[5] T. A. Le and H. D. Nguyen, New multiple insertion/deletion correcting codes for non-binary alphabets, *IEEE Trans. Inform. Theory* ***62*** (2016), 2682–2693, doi:10.1109/TIT.2016.2541139. MR 3493869 Zbl 1359.94714

[6] D. N. Lehmer, Certain theorems in the theory of quadratic residues, *Amer. Math. Monthly* ***20*** (1913) 151–157, doi:10.2307/2972413. MR 1517830 Zbl 44.0248.09

[7] V. I. Levenshtein, Binary codes capable of correcting deletions, insertions, and reversals, *Soviet Physics Dokl.* ***10*** (1966) 707–710. MR 189928 Zbl 0149.15905

[8] R. R. Varshamov and G. M. Tenengol'ts, Code correcting single asymmetric errors, *Avtomat. i Telemeh.* ***26*** (1965) 288–292. MR 172738