

PERFECT CODES ON SOME ORDERED SETS

JEH GWON LEE

ABSTRACT. Using the concept of codes on ordered sets introduced by Brualdi, Graves and Lawrence, we consider perfect codes on the ordinal sum of two ordered sets, the standard ordered sets and the disjoint sum of two chains.

In the classical coding theory all perfect codes are completely described in terms of parameters (cf. [2, 3]). They are mathematically interesting structures. Brualdi et al. [1] recently introduced the notion of a code on an ordered set. In this paper we consider perfect codes on the ordinal sum of two ordered sets, the standard ordered sets and the disjoint sum of two chains.

A *chain* is an ordered set in which every two elements are comparable and an *antichain* in which no two elements are comparable. Then we denote by \mathbf{n} and \underline{n} denote the chain and the antichain, respectively, on the set $\{1, 2, \dots, n\}$. Let P and Q be two disjoint ordered sets. The *disjoint sum* $P + Q$ of P and Q is the ordered set on $P \cup Q$ such that $x < y$ if and only if $x, y \in P$ and $x < y$ in P or $x, y \in Q$ and $x < y$ in Q , and the *ordinal sum* $P \oplus Q$ of P and Q is obtained from $P + Q$ by adding the new relations $x < y$ for all $x \in P$ and $y \in Q$.

Let \mathbb{F}_q be a finite field with $q = p^d$ (p a prime, d a positive integer). For $u = (u_1, \dots, u_n) \in \mathbb{F}_q^n$, the support of u and the Hamming weight of u are respectively given by

$$\text{Supp}(u) = \{i : 1 \leq i \leq n, u_i \neq 0\},$$

$$w_H(u) = |\text{Supp}(u)|.$$

Received December 30, 2004.

2000 Mathematics Subject Classification: 94B05.

Key words and phrases: perfect code, ordered set.

This work was supported by the Sogang University Grant in 2003.

Brualdi et al. [1] generalized the notion of Hamming weight to that of P -weight, where P is an ordered set on the set of coordinate positions of vectors in \mathbb{F}_q^n . For such a P , the P -weight $w_P(u)$ of $u \in \mathbb{F}_q^n$ is defined to be

$$w_P(u) = |\langle \text{Supp}(u) \rangle|,$$

where $\langle \text{Supp}(u) \rangle$ denotes the smallest ideal containing $\text{Supp}(u)$. (Recall a subset I of an ordered set is an *ideal* if $a \in I$ and $b < a \Rightarrow b \in I$.) Now one can show that P -distance $d_P(u, v) = w_P(u - v)$ is a metric on \mathbb{F}_q^n . If P is an antichain, then P -weight and P -distance are, respectively, Hamming weight and Hamming distance of classical coding theory. If \mathbb{F}_q^n is endowed with P -distance, then a subset C of \mathbb{F}_q^n is called a *code on P over \mathbb{F}_q* . Let x be a vector in \mathbb{F}_q^n and r be a nonnegative integer. The P -sphere with center x and radius r is the set

$$S_P(x; r) = \{y \in \mathbb{F}_q^n : d_P(x, y) \leq r\}.$$

Then C is called a *perfect code on P over \mathbb{F}_q* provided there exists an integer r such that the P -spheres of radius r with centers at the codewords of C are pairwise disjoint and their union is \mathbb{F}_q^n .

LEMMA 1. *Let C be a perfect code on an ordered set over \mathbb{F}_q . Then the number of codewords of C is a power of q .*

Proof. Cf. Lemma 34 [2]. □

First we characterize perfect codes on the ordinal sum of two ordered sets. From now on, we use $x_1x_2 \cdots x_n$ instead of the usual vector notation (x_1, x_2, \dots, x_n) . So, for $x = x_1x_2 \cdots x_m \in \mathbb{F}_q^m$ and $y = y_1y_2 \cdots y_n \in \mathbb{F}_q^n$, we write $xy = x_1x_2 \cdots x_my_1y_2 \cdots y_n \in \mathbb{F}_q^{m+n}$. In the following theorem, for $x \in \mathbb{F}_q^m$ and $y \in \mathbb{F}_q^n$, xy means that x has its coordinate positions on P and y has its coordinate positions on P' .

THEOREM 1. *Let P and P' be ordered sets with $|P| = m$ and $|P'| = n$, respectively. Then every perfect code C on $P \oplus P'$ over \mathbb{F}_q satisfies one of the following:*

- (i) $|C| \geq q^n$ and, for each $y \in \mathbb{F}_q^n$, $\{x \in \mathbb{F}_q^m : xy \in C\}$ is a perfect code on P of the same size.
- (ii) $|C| < q^n$ and $C = \{x_y y : y \in C_0\}$, where C_0 is a perfect code on P' and $y \mapsto x_y$ is a map from C_0 into \mathbb{F}_q^m .

Proof. Let C be a perfect code on $Q = P \oplus P'$ over \mathbb{F}_q . Then $|C| = q^k$ for some k by Lemma 1. Suppose that the Q -spheres of radius r with centers at the codewords of C are pairwise disjoint and their union is \mathbb{F}_q^{m+n} . Now we have two cases to consider.

(i) If $k \geq n$, then $|S_Q(x; r)| \leq q^m$ and so $r \leq m$. For any $y \in \mathbb{F}_q^n$, there exists $x \in \mathbb{F}_q^m$ such that $xy \in C$. For, if there is $y \in \mathbb{F}_q^n$ such that $xy \notin C$ for any $x \in \mathbb{F}_q^m$, then $d_Q(xy, c) > m \geq r$ for any $c \in C$, which is a contradiction. Now, for each $y \in \mathbb{F}_q^n$, $\{x \in \mathbb{F}_q^m : xy \in C\}$ is a perfect code on P of the same size.

(ii) If $k < n$, then $|S_Q(x; r)| > q^m$ and so $r > m$. If $x \neq x'$ and $xy, x'y \in C$ for $x, x' \in \mathbb{F}_q^m$, $y \in \mathbb{F}_q^n$, then $d_Q(xy, x'y) \leq m$ and so $r \leq m$, which is a contradiction. \square

COROLLARY 1. [1] *Let $P = \underline{n}$. Then C is a perfect code on P over \mathbb{F}_q if and only if there exists an integer k with $0 \leq k \leq n$ such that $|C| = q^k$ and the set of all vectors $x_{n-k+1} \cdots x_n$ such that $x_1 \cdots x_n \in C$ for some $x_1 \cdots x_{n-k} \in \mathbb{F}_q^{n-k}$ equals to \mathbb{F}_q^k .*

COROLLARY 2. [1] *Let $P_n = \underline{1} \oplus \underline{n}$. Then, for each positive integer m , the extended binary Hamming code with parameters $[n = 2^m, 2^m - m - 1, 4]$ is a perfect code on P_{n-1} . In addition, the extended binary Golay code with parameters $[24, 12, 8]$ is a perfect code on P_{23} , and the extended ternary Golay code with parameters $[12, 6, 6]$ is a perfect code on P_{11} .*

Let $\mathcal{P}(X)$ be the power set of a set X with $|X| = n$. For a natural number $n \geq 3$, consider the ordered set $S_n = (\{A \in \mathcal{P}(X) : |A| \in \{1, n-1\}\}, \subseteq)$, which is usually called the n -dimensional standard ordered set. Now we have a similar result to Theorem 1 for these important ordered sets. Here, for $x, y \in \mathbb{F}_q^n$, xy means that x has its coordinate positions on the minimal elements of S_n and y has its coordinate positions on the maximal elements of S_n .

THEOREM 2. *For an integer $n \geq 3$, there is no perfect code C on S_n with $|C| = q^n$. Otherwise, every perfect code C on S_n satisfies one of the following:*

(i) $|C| > q^n$ and, for each $y \in \mathbb{F}_q^n$, $\{x \in \mathbb{F}_q^n : xy \in C\}$ is a perfect code on the set of all minimal elements of S_n of the same size.

(ii) $|C| < q^n$ and $C = \{x_y y : y \in C_0\}$, where C_0 is a perfect code on the set of all maximal elements of S_n and $y \mapsto x_y$ is a map from C_0 into \mathbb{F}_q^n .

Proof. Since $|S_{S_n}(x; r)| < q^n$ for $r < n$ and $|S_{S_n}(x; n)| = q^n + n(q - 1)q^{n-1}$, there is no S_n -sphere of size q^n , whence there is no perfect code C on S_n with $|C| = q^n$. Now the rest of proof is similar to that of Theorem 1. \square

Brualdi et al. [1] showed that there is no nontrivial perfect code on a disjoint sum of two chains of the same size. This is still true for a disjoint sum of two chains of different sizes.

THEOREM 3. *For any positive integers m and n , there is no nontrivial perfect code on $\mathbf{m} + \mathbf{n}$.*

Proof. Let $P = \mathbf{m} + \mathbf{n}$ with $m \geq n \geq 1$, where $\mathbf{m} = \{1 < 2 < \dots < m\}$ and $\mathbf{n} = \{1' < 2' < \dots < n'\}$. Suppose that C a nontrivial perfect code on P and that the P -spheres of radius r with centers at the codewords of C are pairwise disjoint and their union is \mathbb{F}_q^{m+n} . Then we have two cases to consider.

Case 1. $r \geq m$.

Let $x = x_1 \dots x_m x_{1'} \dots x_{n'}$ and $y = y_1 \dots y_m y_{1'} \dots y_{n'}$ be any two codewords of C . Then the vector $x_1 \dots x_m y_{1'} \dots y_{n'}$ is contained in $S_P(x; r) \cap S_P(y; r)$, contradicting the assumption that C is perfect.

Case 2. $r < m$.

Set $l = \min\{r, n\}$. For $x = x_1 \dots x_m x_{1'} \dots x_{n'} \in C$, let $B_0 = \{y_1 \dots y_m y_{1'} \dots y_{n'} \in S_P(x; r) : y_{i'} = x_{i'}, 1 \leq i \leq n\}$ and $B_i = \{y_1 \dots y_m y_{1'} \dots y_{n'} \in S_P(x; r) : y_{i'} \neq x_{i'}, y_{j'} = x_{j'}, i < j \leq l\}$ for $1 \leq i \leq l$. Clearly, $|B_0| = q^r$ and, for $1 \leq i \leq l$, $|B_i| = (q - 1)q^{r-1}$. Now,

$$\begin{aligned} |S_P(x; r)| &= \sum_{i=0}^l |B_i| = l(q - 1)q^{r-1} + q^r < q^{r-1}(l + 1)q \\ &\leq q^{r-1}q^{l+1} = q^{r+l}. \end{aligned}$$

Hence, $|C| > q^{m-r}$ when $n \leq r$, i.e., $l = n$. By the pigeon-hole principle, there exist two distinct codewords $x = x_1 \dots x_m x_{1'} \dots x_{n'}$ and $y = y_1 \dots y_m y_{1'} \dots y_{n'}$ such that $x_i = y_i$ for $m \geq i > r$. Similarly, $|C| > q^{m+n-2r}$ when $r < n$, i.e., $l = n$. Again, there exist two distinct codewords $x = x_1 \dots x_m x_{1'} \dots x_{n'}$ and $y = y_1 \dots y_m y_{1'} \dots y_{n'}$ such that $x_i = y_i$ for $m \geq i > r$ and $x_{i'} = y_{i'}$ for $n \geq i > r$. In both cases, the vector $x_1 \dots x_m y_{1'} \dots y_{n'}$ is contained in $S_P(x; r) \cap S_P(y; r)$, which also contradicts the assumption that C is perfect. \square

References

- [1] R. A. Brualdi, J. Graves and K. M. Lawrence, *Codes with a poset metric*, Discrete Math. **147** (1995), no. 1-2, 57–72.
- [2] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes I, II*, North-Holland, Amsterdam, 1977.
- [3] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1998.

DEPARTMENT OF MATHEMATICS, SOGANG UNIVERSITY, SEOUL 121-742, KOREA
E-mail: ljg@sogang.ac.kr