Distance theorems for code pairs

Distance Theorems for Code Pairs

J. H. VAN LINT

Department of Mathematics and Computing Science
Eindhoven University of Technology
Eindhoven, The Netherlands

INTRODUCTION

We shall report on recent results (by several authors) on problems concerning the distances of code words, where the words are from two binary codes A and B of length n. In the first two problems we suppose that there is a number δ such that $d(\mathbf{a}, \mathbf{b}) = \delta$ for every $\mathbf{a} \in A$ and every $\mathbf{b} \in B$. In [1] Ahlswede *et al.* proved that this condition implies that $|A| \cdot |B| \leq 2^{2\lfloor n/2 \rfloor}$. Although their proof is not long, it is not simple. We give a practically trivial proof of the same theorem and discuss the case of equality (cf. [3]). Next, we consider the same problem but with δ prescribed. Recently, it was shown by Van Pul [7] that we then have

$$|A| \cdot |B| \leq \max \left\{ 2^{2i} \binom{n-2i}{\delta - i} \,\middle|\, 0 \leq i \leq \delta \right\}.$$

He also characterized the case of equality.

The third problem is of a different nature. Again A and B are binary codes of length n. In a long paper, Körner and Wei [5] considered several problems of the following kind. Given some distance property of A and B, can we replace A and B by "spheres" of the same cardinality with a similar property? Here, by a sphere of cardinality k we mean a subset S of the Hamming sphere $S_{\rho+1}(\mathbf{x}) := \{\mathbf{y} \in \mathbb{F}_2^n \mid d(\mathbf{x}, \mathbf{y}) \leq \rho + 1\}$ such that $S_\rho(\mathbf{x}) \subseteq S$ and $|S| = k$. In the problem that we are interested in, S is replaced by a "pure parity sphere" S', which is the subset of S consisting of all the words whose weights have the same parity as the center of S. In [5] Körner and Wei proved that if the codes A and B both have distance at least 2, then there exist pure parity spheres $\hat{A}$ and $\hat{B}$ centered at $\mathbf{1}$ respectively $\mathbf{0}$, such that $|\hat{A}| = |A|$, $|\hat{B}| = |B|$, and $d(\hat{A}, \hat{B}) \geq d(A, B)$. We present a very short proof of this theorem, which is due to Tiersma [6].

CONSTANT DISTANCE CODE PAIRS

Consider a constant distance code pair, that is, a pair of binary codes A, B, of length n such that for some integer δ we have $d(\mathbf{a}, \mathbf{b}) = \delta$ for every $\mathbf{a} \in A$ and every $\mathbf{b} \in B$. We shall show that A and B are translates of a pair of orthogonal codes. If we consider the words $\mathbf{a}$ and $\mathbf{b}$ as vectors in $\mathbb{Z}^n$, then we have

$$2(\mathbf{a}, \mathbf{b}) = wt(\mathbf{a}) + wt(\mathbf{b}) - \delta,$$

and in particular, it follows that the weights of the words of A (respectively B) all have the same parity. Furthermore, for code words $\mathbf{a}_i \in A$, $\mathbf{b}_i \in B$, $(i = 1, 2)$, we have

$$wt(\mathbf{a}_1) + wt(\mathbf{a}_2) + wt(\mathbf{b}_1) + wt(\mathbf{b}_2) - 2\delta = (\mathbf{a}_1 + \mathbf{a}_2, \mathbf{b}_1 + \mathbf{b}_2).$$

Interpreting this over $\mathbb{F}_2^n$ shows that the sum of any two words from A is orthogonal to the sum of any two words from B. Fixing $\mathbf{a}_1$ and $\mathbf{b}_1$, we see that $\mathbf{a}_1 + A$ and $\mathbf{b}_1 + B$ are even weight orthogonal codes. This proves the following theorem.

THEOREM 1: If A and B are a constant distance code pair of length n, then

$$|A| \cdot |B| \leq 2^{2\lfloor n/2 \rfloor}.$$

With only slightly more difficulty, it is shown in [3] that equality only holds in the following cases:

(i) $n = 2m$, $\quad A = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \mathbb{F}_2^m\}$,
$\quad B = \{(\mathbf{y}, \mathbf{1} + \mathbf{y}) \mid \mathbf{y} \in \mathbb{F}_2^m\}$;

(ii) $n = 2m + 1$, $\quad A$ and B as in (i), but both extended by a fixed bit.

So we see that equality in Theorem 1 implies that the constant distance is equal to $\lfloor n/2 \rfloor$ or $\lfloor (n+1)/2 \rfloor$. Suppose we fix δ a priori and consider the same problem. One obvious way of making a constant distance code pair A, B is to take $A = \{\mathbf{0}\}$ and to let B consist of all words of weight δ. We now combine this idea with the case of equality in Theorem 1 as follows. For the first $2i$ bits of A and B, we proceed as was done for a constant distance code pair of distance i. On the final $n - 2i$ bits we take A to be $\mathbf{0}$ and B to have weight $\delta - i$. Then A has cardinality 2^i and B has cardinality $2^i \binom{n-2i}{\delta - i}$. For this constant distance code pair we have

$$|A| \cdot |B| = 2^{2i} \binom{n-2i}{\delta - i}.$$

We define

$$M(n, \delta) := \max \{|A| \cdot |B| \mid (A, B) \text{ a constant distance } \delta \text{ code pair of length } n\}.$$

THEOREM 2: We have

$$M(n, \delta) = \max \left\{ 2^{2i} \binom{n-2i}{\delta - i} \,\middle|\, 0 \leq i \leq \delta \right\}.$$

Proof ([7]): In the following A, B is a constant distance δ code pair of length n such that $|A| \cdot |B| = M(n, \delta)$. If $1 \leq i < j \leq n$, we define α_{ij} to be the number of pairs $\{\mathbf{a}, \mathbf{b}\}$ with $\mathbf{a} \in A$, $\mathbf{b} \in B$, such that these words differ in exactly one of the positions i, j. It follows that

$$\sum_{0 \leq i < j \leq n} \alpha_{ij} = \delta(n - \delta) \cdot |A| \cdot |B| = \delta(n - \delta) \cdot M(n, \delta). \tag{1}$$

From (1) we find that there is a pair i, j such that

$$\alpha_{ij} \geq \delta(n - \delta) \cdot M(n, \delta) \Big/ \binom{n}{2} \tag{2}$$

and from now on we take this pair to be $i = 1, j = 2$ (w.l.o.g.). We use the following notation:

A_{00} = the code of length $n-2$ obtained from A by taking the words starting with 00 and deleting these bits.

(Similarly for other indices and for B.) The following observation is trivial:

$(A_{00} \cup A_{11}, B_{01} \cup B_{10})$ is a constant distance $\delta - 1$ code pair of length $n-2$. (3)

Furthermore we clearly have

$$\alpha_{12} = (|A_{00}| + |A_{11}|)(|B_{01}| + |B_{10}|) + (|A_{01}| + |A_{10}|)(|B_{00}| + |B_{11}|). \quad (4)$$

The analysis of this relation depends on whether some of the factors are 0 or not. So we make the following simple observation.

If $A_{00} \cap A_{11} \neq \varnothing$, then B_{00} and B_{11} must both be empty and because of the maximality of $|A| \cdot |B|$, we then must have $A_{00} = A_{11}$. (Similar assertions are obviously true for other choices of index pairs and if we interchange A and B.) (5)

We now analyze (4) and distinguish three cases.

Case I: $A_{00} \cap A_{11} \neq \varnothing$ and $B_{01} \cap B_{10} \neq \varnothing$. By (5) we have

$$M(n, \delta) = |A| \cdot |B| = \alpha_{12} = (|A_{00}| + |A_{11}|)(|B_{01}| + |B_{10}|)$$
$$= 4|A_{00}| \cdot |B_{01}|$$

and then (3) yields

$$M(n, \delta) \leq 4M(n-2, \delta - 1). \quad (6)$$

Case II: $A_{00} \cap A_{11} \neq \varnothing$ and $B_{01} \cap B_{10} = \varnothing$. As previously, we find

$$\alpha_{12} = (|A_{00}| + |A_{11}|)(|B_{01}| + |B_{10}|)$$
$$= 2|A_{00}| \cdot |B_{01} \cup B_{10}| \leq 2M(n-2, \delta - 1).$$

Case III: If all relevant intersections are empty, then (3) and (5) yield

$$\alpha_{12} = |A_{00} \cup A_{11}| \cdot |B_{01} \cup B_{10}| + |A_{01} \cup A_{10}| \cdot |B_{00} \cup B_{11}|$$
$$\leq 2M(n-2, \delta - 1).$$

Combining the last two cases and (2) yields

$$M(n, \delta) \leq \frac{n(n-1)}{\delta(n-\delta)} M(n-2, \delta - 1). \quad (7)$$

Finally, combining (6) and (7) yields the following lemma.

LEMMA 1: We have

$$M(n, \delta) \leq \max\left\{4, \frac{n(n-1)}{\delta(n-\delta)}\right\} M(n, \delta - 1), \qquad 1 \leq \delta \leq \frac{n}{2}.$$

It is now an easy exercise (which we leave to the reader) to show that Theorem 2 follows from Lemma 1 by induction (or see [7]).

In [7] arguments similar to those previously given, again with a distinction between several cases, are used to show that the code pairs just constructed, which achieve the bound of Theorem 2, are essentially the only codes for which this is true.

CODE PAIRS AND SPHERES

For the definition of a pure parity sphere S' of cardinality k centered at $\mathbf{x}$ we refer the reader to the first section.

THEOREM 3: Let A and B be binary codes of length n, each with minimum distance at least 2. There exist pure parity spheres $\hat{A}$ and $\hat{B}$ centered at $\mathbf{1}$ respectively $\mathbf{0}$ such that $|\hat{A}| = |A|, |\hat{B}| = |B|$, and $d(\hat{A}, \hat{B}) \leq d(A, B)$.

Proof: We first observe that if we had left out the pure parity condition, then Theorem 3 would become equivalent to a theorem of Harper [4] for which Frankl and Füredi [2] recently gave a simple proof. From each A and B we now obtain the codes A^* and B^* by deleting the first coordinate. Clearly, $d(A^*, B^*) \geq d(A, B) - 1$. By Harper's theorem there are spheres $\hat{A}^*$ and $\hat{B}^*$ centered at $\mathbf{1}$ respectively $\mathbf{0}$ such that $d(\hat{A}^*, \hat{B}^*) \geq d(A^*, B^*)$, while $|\hat{A}^*| = |A^*|$ and $|\hat{B}^*| = |B^*|$. Now suppose $d(A, B)$ is odd (the even case is similar). Extend all words in $\hat{A}^*$ by a bit, which makes their weights even, and similarly extend $\hat{B}^*$ to make all weights odd. If the extended codes are $\hat{A}$ and $\hat{B}$, then $d(\hat{A}, \hat{B})$ is odd. Therefore, $d(\hat{A}, \hat{B}) \geq d(A^*, B^*) \geq d(A, B) - 1$ implies that $d(\hat{A}, \hat{B}) \geq d(A, B)$. Furthermore, $\hat{A}$ and $\hat{B}$ are pure parity spheres of the required cardinality. □

Besides this proof, Tiersma [6] gives two other short proofs of results from [4].

REFERENCES

1. AHLSWEDE, R., A. EL GAMAL & K. F. PANG. 1984. A two-family extremal problem in Hamming space. Discrete Math. **49**: 1–5.
2. FRANKL, P. & Z. FÜREDI. 1981. A short proof of a theorem of Harper about Hamming-spheres. Discrete Math. **39**: 311–313.
3. HALL, J. I. & J. H. VAN LINT. 1985. Constant distance code pairs. Proc. Kon. Ned. Akad. Wet. (A) **88**(1): 41–45.
4. HARPER, K. H. 1966. Optimal numberings and isoperimetric problems on graphs. J. Comb. Theory **1**: 385–393.
5. KÖRNER, J. & V. K. WEI. 1984. Odd and even Hamming spheres also have minimum boundary. Discrete Math. **51**: 147–165.
6. TIERSMA, H. J. 1985. A note on Hamming spheres. Discrete Math. **54**: 225–228.
7. VAN PUL, C. L. M. Constant distance code pairs. Proc. Kon. Ned. Akad. Wet. In press.