Journal of Combinatorial Theory, Series A 116 (2009) 1087–1096

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Note

On the size of identifying codes in binary hypercubes

Svante Janson [a], Tero Laihonen [b,1]

[a] Department of Mathematics, Uppsala University, PO Box 480, SE-751 06 Uppsala, Sweden
[b] Department of Mathematics, University of Turku, FIN-20014 Turku, Finland

ARTICLE INFO

Article history:
Received 18 April 2008
Available online 28 March 2009

Keywords:
Identifying code
Optimal rate
Hypercube
Fault diagnosis

ABSTRACT

In this paper, we consider identifying codes in binary Hamming spaces $\mathbb{F}^n$, i.e., in binary hypercubes. The concept of $(r, \leqslant \ell)$-identifying codes was introduced by Karpovsky, Chakrabarty and Levitin in 1998. Currently, the subject forms a topic of its own with several possible applications, for example, to sensor networks.

Let us denote by $M_r^{(\leqslant \ell)}(n)$ the smallest possible cardinality of an $(r, \leqslant \ell)$-identifying code in $\mathbb{F}^n$. In 2002, Honkala and Lobstein showed for $\ell = 1$ that

$$\lim_{n\to\infty} \frac{1}{n} \log_2 M_r^{(\leqslant \ell)}(n) = 1 - h(\rho),$$

where $r = \lfloor \rho n \rfloor$, $\rho \in [0, 1)$ and $h(x)$ is the binary entropy function. In this paper, we prove that this result holds for any fixed $\ell \geqslant 1$ when $\rho \in [0, 1/2)$. We also show that $M_r^{(\leqslant \ell)}(n) = O(n^{3/2})$ for every fixed ℓ and r slightly less than $n/2$, and give an explicit construction of small $(r, \leqslant 2)$-identifying codes for $r = \lfloor n/2 \rfloor - 1$.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F} = \{0, 1\}$ be the binary field and denote by $\mathbb{F}^n$ the n-fold Cartesian product of it, i.e., the Hamming space. We denote by $A \triangle B$ the *symmetric difference* $(A \setminus B) \cup (B \setminus A)$ of two sets A and B. The (*Hamming*) *distance* $d(x, y)$ between the vectors (called words) $x, y \in \mathbb{F}^n$ is the number of coordinate places in which they differ, i.e., $x(i) \neq y(i)$ for $i = 1, 2, \dots, n$. The *support* of $x = (x(1), x(2), \dots, x(n)) \in \mathbb{F}^n$ is defined by $\mathrm{supp}(x) = \{i \mid x(i) = 1\}$. The *complement* of a word $x \in \mathbb{F}^n$, denoted by $\bar{x}$, is the word for which $\mathrm{supp}(\bar{x}) = \{1, 2, \dots, n\} \setminus \mathrm{supp}(x)$. Denote by 0 the word where all the coordinates equal zero, and by 1 the all-one word. Clearly $\bar{0} = 1$. The (*Hamming*) *weight* $w(x)$

E-mail address: terolai@utu.fi (T. Laihonen).

[1] Research supported by the Academy of Finland under grant 111940.

0097-3165/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2009.02.004

of a word $x \in \mathbb{F}^n$ is defined by $w(x) = d(x, 0) = |\mathrm{supp}(x)|$. We say that x *r-covers* y if $d(x, y) \leqslant r$ (if x r-covers y, then also y r-covers x). The (*Hamming*) *ball* of radius r centered at $x \in \mathbb{F}^n$ is

$$B_r(x) = \{ y \in \mathbb{F}^n \mid d(x, y) \leqslant r \}$$

and its cardinality is denoted by $V(n, r)$. For $X \subseteq \mathbb{F}^n$, denote

$$B_r(X) = \bigcup_{x \in X} B_r(x) = \{ y \in \mathbb{F}^n \mid d(y, X) \leqslant r \}.$$

We also use the notation

$$S_r(x) = \{ y \in \mathbb{F}^n \mid d(x, y) = r \}.$$

A nonempty subset $C \subseteq \mathbb{F}^n$ is called a *code* and its elements are *codewords*. Let C be a code and $X \subseteq \mathbb{F}^n$. We denote (the codeword r-neighbourhood of X by)

$$I_r(X) = I_r(C; X) = B_r(X) \cap C.$$

We write for short $I_r(C; \{x_1, \ldots, x_k\}) = I_r(x_1, \ldots, x_k)$.

Definition 1. Let r and ℓ be non-negative integers. A code $C \subseteq \mathbb{F}^n$ is said to be $(r, \leqslant \ell)$*-identifying* if for all $X, Y \subseteq \mathbb{F}^n$ such that $|X| \leqslant \ell$, $|Y| \leqslant \ell$ and $X \neq Y$ we have

$$I_r(C; X) \neq I_r(C; Y).$$

The idea of the identifying codes is that given the set $I_r(X)$ we can uniquely determine the set $X \subseteq \mathbb{F}^n$ as long as $|X| \leqslant \ell$.

The seminal paper [15] by Karpovsky, Chakrabarty and Levitin initiated research in identifying codes, and it is nowadays a topic of its own with different types of problems studied, see, e.g., [2,4–6,11,12,20,22]; for an updated bibliography of identifying codes see [19]. Originally, identifying codes were designed for finding malfunctioning processors in multiprocessor systems (such as binary hypercubes, i.e., binary Hamming spaces); in this application we want to determine the set of malfunctioning processors X of size at most ℓ when the only information available is the set $I_r(C; X)$ provided by the code C. A natural goal there is to use identifying codes which are as small as possible. The theory of identification can also be applied to sensor networks, see [21]. Small identifying codes are needed for energy conservation [16]. For other applications we refer to [17].

The smallest possible cardinality of an $(r, \leqslant \ell)$-identifying code in $\mathbb{F}^n$ is denoted by $M_r^{(\leqslant \ell)}(n)$.

Let $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ be the binary entropy function and $\rho \in [0, 1)$ be a constant. Let further $r = \lfloor \rho n \rfloor$. Honkala and Lobstein showed in [14] that, when $\ell = 1$, we have

$$\lim_{n \to \infty} \frac{1}{n} \log_2 M_r^{(\leqslant 1)}(n) = 1 - h(\rho). \tag{1}$$

The lower bound that is part of (1) comes from the simple observation that if C is an $(r, \leqslant \ell)$-identifying code for any $\ell \geqslant 1$, then necessarily $B_r(C) = \mathbb{F}^n$ (otherwise there would be a word $x \notin B_r(C)$ and then $I_r(x) = \emptyset = I_r(\emptyset)$, so $\{x\}$ and $\emptyset$ cannot be distinguished by C) and also $|\mathbb{F}^n \setminus B_{n-r-1}(C)| \leqslant 1$ (otherwise there would be two words $x, y \notin B_{n-r-1}(C)$ and then $I_r(\bar{x}) = C = I_r(\bar{y})$, so $\{\bar{x}\}$ and $\{\bar{y}\}$ cannot be distinguished by C); consequently, for any $n, r, \ell \geqslant 1$,

$$\begin{aligned} M_r^{(\leqslant \ell)}(n) \geqslant M_r^{(\leqslant 1)}(n) &\geqslant \max\left(\frac{2^n}{|V(n,r)|}, \frac{2^n - 1}{|V(n, n-r-1)|} \right) \\ &= \max\left(\frac{2^n}{\sum_{i=0}^{r} \binom{n}{i}}, \frac{2^n - 1}{\sum_{i=0}^{n-r-1} \binom{n}{i}} \right) \end{aligned} \tag{2}$$

and the lower bound in (1) follows from Stirling's formula. Cf. [7, Chapter 12], [3,10,14,15] for this and similar arguments and related estimates.

Download English Version:

https://daneshyari.com/en/article/4656215

Download Persian Version:

https://daneshyari.com/article/4656215

Daneshyari.com