Minimal Vectors in Linear Codes and Sharing of Secrets *

Alexei Ashikhmin[†] Alexander Barg[†, ‡]

We study access structures in secret sharing schemes determined by linear codes. They are known to be characterized by the set of minimal codewords (in essence, by the set of minimal supports of the codewords). After stating some simple properties of these sets, we find them for random linear codes, the Hamming codes, and second-order Reed–Muller codes. We also extend the concept of linear secret-sharing schemes to certain finite rings.

Keywords – Ideal secret-sharing schemes, vector matroids, minimal codewords.

1 Introduction

The concept of secret sharing has been recently extensively discussed in cryptography (an overview and relevant references are found in [1]). Informally, this concept can be described as follows. A center D has to create a system of distributed access to a certain information s_0. Toward this end, it gives out to the users in the set $\mathcal{U} = \{p_1, \ldots, p_{n-1}\}$ of the system some portions (shares) of information. The goal of the center is to ensure that only the authorized coalitions of users, putting their shares together, can learn s_0, while all other (unauthorized) coalitions can obtain from their joint knowledge as little information about s_0 as possible. In *perfect secret-sharing schemes*, this illegal information is required to be void. Suppose the shares $s_i, 1 \le i \le n-1$, and the value s_0 are taken from a finite set S (thus, we confine ourselves to *ideal* secret-sharing schemes in which the information rate $R \triangleq \max_i(\log s_i/\log s_0)$ always equals 1). The collection of authorized coalitions is called an access structure (denoted $\Gamma, \Gamma \subseteq 2^{\mathcal{U}}$). It is natural (though not necessary) to assume that if a certain coalition can learn s_0 then this property is not damaged by

*The results of this paper were presented in part at the Fourth International Workshop "Algebraic and Combinatorial Coding Theory" (ACCT-4), Novgorod, 11–17 September 1994.

†Institute for Information Transmission Problems, 19 Ermolovoi st., Moscow GSP-4, 101447.

‡Faculty of Mathematics and Computer Science, University of Technology, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven. The research of this author was partially supported by the International Science Foundation under grant MEF000.

adding extra users to it. Such access structures, for which $\gamma_1 \in \Gamma$ and $\gamma_1 \subset \gamma_2$ imply $\gamma_2 \in \Gamma$, are called *monotone*. Thus, what we really need to study is the *minimal* (or Sperner) access structure, i.e., the maximal set $\Gamma^- \subseteq \Gamma$ with the property that $\gamma_1, \gamma_2 \in \Gamma^-$ implies that neither $\gamma_1 \subseteq \gamma_2$ nor $\gamma_2 \subseteq \gamma_1$. An access structure is called *connected* if for any $p \in \mathcal{U}$ there exists a $\gamma \in \Gamma^-$ such that $p \in \gamma$.

The concept of secret sharing was first introduced in [2, 3] (in a particular case) and the general definition was given in [4].

To define a secret-sharing scheme it is necessary to define a set of distribution rules, i.e., of functions that assign shares to the users. If S is a finite field and those functions are linear over it, the scheme is called *linear*. Linear schemes, which form the subject of this paper, were studied in [5]–[9]

Formal definitions and a relation to error-correcting codes are given in Secs. 2, 3. This relation shows [6, 7] that the access structure of a linear secret-sharing scheme is determined by the set of so-called minimal codewords of an associated linear code, i.e., of codewords that cover no other noncollinear codewords in this code. The minimal access structure Γ^- is formed by the users contained in supports of minimal codewords that have a nonzero first coordinate. The entire access structure Γ is formed by all the sets of users that contain the minimal subsets $\gamma \in G^-$. Thus, a natural question[1] is to study which access structures are defined by well-known linear codes. Massey [6] and Blakley and Kabatianskii [7] suggest this question as a research problem. Interestingly, the set of minimal codewords has been studied already in [13] (for decoding purposes). There this set was called the *projecting set* of a code. For a code C, we denote its set of minimal codewords by $\mathcal{P}(C)$ or simply by $\mathcal{P}$. We assume that $\mathbf{0} \notin \mathcal{P}$ and suggest a notation $C^\times \triangleq C - \{\mathbf{0}\}$.

There are many binary codes with $\mathcal{P}(C) = C^\times$. They are called intersecting after [10, 11]. In our setting, if a code is intersecting, then all of its codewords with a nonzero first coordinate define minimal authorized coalitions.

In Sec. 4, we explore properties of minimal codewords and find their number in typical linear codes. The subsequent asymptotic analysis enables us to assess, from the complexity point of view, the decoding algorithm in [13]. We also find $\mathcal{P}(C)$ for C the Hamming code and second-order Reed–Muller code. In Sec. 5, we extend our study to the case of S a Galois ring, when the corresponding secret-sharing schemes turn out to be nonperfect. It also turns out that, especially in connection with rings, it is more accurate to speak of minimal supports (sets of coordinates) rather than of codewords themselves. In binary codes, this difference is hidden.

[1]for a coding theorist, though, probably, not for a cryptologist, who would like to construct a scheme starting from a given access structure rather than to find which structure corresponds to a scheme determined by some considerations foreign to cryptography.