GEOMETRIC SPACES AND EFFICIENT CODES

Luca Tallini

In this paper the theory of geometric spaces is used to construct new efficient error control codes with parallel coding procedures.

1. INTRODUCTION

Let \((S, \mathcal{B})\) be a finite geometric space, i.e. \(S\) is a finite non empty set and \(\mathcal{B}\) is a family of subset of \(S\) whose elements are called blocks. Let \(n = |S|\) and

\[ S = (P_1, P_2, \ldots, P_n) \]

be an ordering of \(S\). The characteristic mapping \(\chi : \mathcal{P}(S) \rightarrow \mathbb{Z}_2^n\) (\(\mathcal{P}(S)\) is the power set of \(S\)) is the function that associates every subset \(X \in \mathcal{P}(S)\) with the vector \(\chi(X) \in \mathbb{Z}_2^n\) whose \(i\)-th component is 1 if \(P_i \in X\) and 0 if \(P_i \notin X\). It is well known that \(\chi\) is an isomorphism between \((\mathcal{P}(S), \triangle, \cap)\) and \((\mathbb{Z}_2^n, +, \cdot)\), where \(\triangle\) is the symmetric difference. In the following, we will identify \(X \in \mathcal{P}(S)\) and \(\chi(X) \in \mathbb{Z}_2^n\).

In \((S, \mathcal{B}), X \in \mathcal{P}(S)\) is called of even type if for all \(B \in \mathcal{B}, |B \cap X|\) is even. \(X \in \mathcal{P}(S)\) is called of odd type if for all \(B \in \mathcal{B}, |B \cap X|\) is odd \([1]\). We denote by \(\mathcal{E} = \mathcal{E}_{(S, \mathcal{B})}\) and \(\mathcal{D} = \mathcal{D}_{(S, \mathcal{B})}\) the family of even and odd type subsets of \(S\) respectively. Let \(\mathcal{H} = \mathcal{H}_{(S, \mathcal{B})} = \mathcal{E} \cup \mathcal{D}\). It is easy to prove that 1) \(\mathcal{H}\) is a linear subspace of \(\mathbb{Z}_2^n\) and 2) \(\mathcal{E}\) is a linear subspace of \(\mathcal{H}\) such that if \(\mathcal{D} \neq \emptyset\) then \(\dim(\mathcal{E}) = \dim(\mathcal{H}) - 1\). An equivalent way of defining \(\mathcal{H}\) is as follows. Let \(b = |\mathcal{B}|, \mathcal{B} = (B_1, B_2, \ldots, B_b)\) and \(M = M_{(S, \mathcal{B})} = (m_{i,j}) \in \mathcal{M}(b \times n)\) be the incidence matrix of \((S, \mathcal{B})\) (i.e. \(m_{i,j} = 1 \iff P_j \in B_i\)). Evidently, the set

\[ \mathcal{H} = \{ X \in \mathbb{Z}_2^n : XM^T \in \{0, 1\} \} \]
is a linear subspace of $\mathbb{Z}_2^n$ and is exactly the set of even-odd type subset of $(S, \mathcal{B})$. Note that in general, if $T$ is a linear subspace of $\mathbb{Z}_2^n$ then the set

$$\mathcal{H} = \{ X \in \mathbb{Z}_2^n : XM^T \in T \}$$

(1)

is a linear subspace of $\mathbb{Z}_2^n$. As noticed in [5] a geometric space $(S, \mathcal{B})$ determines the linear codes $\mathcal{E}$ and $\mathcal{H}$. Vice versa, we note that, given a linear code $C \subseteq \mathbb{Z}_2^n$, there exists a geometric space $(S, \mathcal{B})$ such that $C = \mathcal{E}_{(S,B)}$. In fact, let

$$H = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix}, \quad b_i \in \mathbb{Z}_2^n \quad i = 1, 2, \ldots, r,$n

be the parity check matrix of $C$. The geometric space

$$(S, \mathcal{B}) = \left( (1, 2, \ldots, n), \{ \chi^{-1}(b_1), \chi^{-1}(b_2), \ldots, \chi^{-1}(b_r) \} \right)$$

is such that

$$X \in C \iff XH^T = 0 \iff X \in \mathcal{E}_{(S,B)}.$$

From the application point of view, the problem is to determine those geometric spaces $(S, \mathcal{B})$ such that the linear codes $\mathcal{H}_{(S,B)}$ are efficient; i.e. 1)there exist very fast and simple error correcting or detecting (or both) algorithms and 2)the number of check bits is small with respect to the number of information bits. Obviously, depending on the application, one has to find the best trade-off between 1) and 2). In this paper, we are concerned with this problem. We give some efficient codes related to simple geometric spaces whose decoding algorithms can be implemented in parallel via combinational circuits.

In this paper the following notations are used:

- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{N}$ set of natural numbers
- $w(X)$ weight of $X \in \mathbb{Z}_2^k$
- $S^k_w = \{ X \in \mathbb{Z}_2^k : w(X) = w \}$
- $|S|$ number of elements of the set $S$
- $a \leftarrow \text{Exp}(X)$ compute $\text{Exp}(X)$ and call the result $a$