



Note

Antiblocking decoding

Hans-Joachim Kroll^{a,*}, Rita Vincenti^b^a Zentrum Mathematik, Technische Universität München, 80290 München, Germany^b Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06100 Perugia, Italy

ARTICLE INFO

Article history:

Received 19 January 2009

Received in revised form 4 April 2010

Accepted 8 April 2010

Available online 1 May 2010

Keywords:

Antiblocking system

PD-set

Antiblocking decoding

Permutation decoding

ABSTRACT

Based on the notion of an antiblocking system a new decoding algorithm is developed which is comparable with the permutation decoding algorithm, but more efficient.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

In communication systems, messages are transmitted over a communication channel. During the transmission errors may occur. Therefore decoding, that is, determining which message x was sent when a message y was received, is one of the pivotal problems of coding theory. For applications, quick algorithms are needed.

In 1962, Prange [7] proved that for a t -error-correcting linear code with minimum distance d for every word r there exists an information set I such that for the code word b with $r_i = b_i$ for $i \in I$ the Hamming distance $q(r, b)$ is less than d . He pointed out that, because of this fact, a decoding algorithm using all information sets would work correctly. But, as the number of distinct information sets can be very large, he did not look for an algorithm using distinct information sets. He stated instead a decoding algorithm for cyclic codes that made use only of one information set and a subgroup S of the automorphism group of the code.

Based on these ideas of E. Prange, Mac Williams [6] developed in 1964 the technique of permutation decoding which can be applied not only to cyclic codes, but to any linear code. This technique uses a subset of the automorphism group of the code, a so-called permutation decoding set. A *permutation decoding set* (for short *PD-set*) for a t -error-correcting code C is a set Σ of automorphisms of the code so that every possible error vector of weight t or less can be moved by some member of Σ out of a fixed information set.

Since the permutation decoding algorithm is more efficient the smaller the size $|\Sigma|$ of the PD-set Σ , it is important for the applications to find small PD-sets. A lower bound on the size of a PD-set is given by Gordon [1]. In some cases it happens that the Gordon bound is greater than the size of the automorphism group of the code so that it is necessary to reduce the error-correcting capability of the code if one wants to apply the permutation decoding algorithm (cf. [3]).

There are examples of PD-sets (cf. [2,4]), but up to now there is no known general method to find PD-sets; and in many cases the size of the PD-set is much larger than that of the Gordon bound.

* Corresponding author.

E-mail addresses: kroll@ma.tum.de (H.-J. Kroll), alice@unipg.it (R. Vincenti).

To handle these problems we introduced the notion of an antiblocking system and succeeded in showing that the Gordon bound is not sharp in any case, i.e., there exist parameters n, k, t such that there is no t -error-correcting $[n, k]$ -code having a PD-set which meets the Gordon bound (cf. [5]).

If I is an information set for a t -error-correcting $[n, k]$ -code C and Σ is a t -PD-set then $\mathfrak{A} := \{\sigma_\pi^{-1}(I) \mid \sigma \in \Sigma\}$ (where σ_π denotes the permutation part¹ of σ) is a t -antiblocking system for $\{1, \dots, n\}$, consisting of information sets.

Instead of using the permutations of Σ as in the permutation decoding algorithm we turn our attention back to the starting point of E. Prange, using only the information sets of \mathfrak{A} , so that we come to the notion of an AI-system. An AI-system is a t -antiblocking system consisting of information sets A_i . In this way we get a new decoding algorithm called an *antiblocking decoding algorithm* which is simpler and faster than the permutation decoding algorithm.

If there exists a PD-set then there exists also an AI-system of the same size. But there may exist also AI-systems which are not derived from PD-sets and which are smaller than the known PD-sets. (See Example at the end of Section 3.)

A comparison of the permutation decoding algorithm and the antiblocking decoding algorithm shows that (even if the size of both systems is the same) the antiblocking decoding needs less computing steps than the permutation decoding. The decisive advantage for the antiblocking decoding however is that it may be applied even if there does not exist a PD-set (i.e., the permutation decoding algorithm is not applicable) or if there exists only a PD-set of very large size but an AI-system of smaller size.

Concerning the question how to find small AI-systems we refer to [5] where we established some properties of antiblocking systems. In particular Lemmas 3, 4 and 6 may help to construct small AI-systems.

2. Linear codes

For the convenience of the reader, and in order to establish our notation we will recall the basic definitions.

Let q be a prime power, let $F = \text{GF}(q)$ be the Galois field of order q and let $n \in \mathbb{N}$. A *linear code* C of length n is a vector subspace of the vector space F^n . For $\mathbf{x} \in F^n$ the set $\text{supp}(\mathbf{x}) := \{i \in \mathbb{N} \mid i \leq n, x_i \neq 0\}$ is called the *support* of \mathbf{x} , and the number $\text{wt}(\mathbf{x}) := |\text{supp}(\mathbf{x})|$ is called the *weight* of \mathbf{x} .

A linear code C of length n is called an $[n, k, d]$ -code, if $k = \dim C$ is the dimension of C and $d = \min\{\text{wt}(\mathbf{c}) \mid \mathbf{c} \in C, \mathbf{c} \neq 0\}$ is the *minimum weight* of C .

For any positive integer t , $t \leq \frac{d-1}{2}$ the code C is a t -error-correcting code.

Since we will use more than one information set it makes no sense to fix an information set and to use the standard form of a linear code. Furthermore, it is necessary to consider the syndrome with respect to any information set. Therefore we introduce the following notation.

Let $C \subset F^n$ be a linear $[n, k, d]$ -code. Every linear bijection $\gamma : F^k \rightarrow C, \mathbf{x} \mapsto \gamma(\mathbf{x})$ is called an *encoder*, and every linear mapping $\kappa : F^n \rightarrow F^l$ (where $|l| = n - k$) with $\text{Kern} \kappa = C$ is called a *check mapping*.

For $I \subset \{1, \dots, n\}$ let

$$p_I : F^n \rightarrow F^I, \mathbf{x} \mapsto \mathbf{x}|_I : \begin{cases} I & \rightarrow F \\ i & \mapsto x_i \end{cases}$$

be the I -projection of F^n .

I is called an *information set* for C if $|I| = k$ and $p_I(C) = F^I$. For any information set I the restriction $p_I|_C$ of p_I on C is a bijection. Therefore, for any encoder $\gamma : F^k \rightarrow C$ the linear mapping $p_I \gamma : F^k \rightarrow F^I$ is a bijection.

For $I \subset \{1, \dots, n\}$ let $I' := \{1, \dots, n\} \setminus I$.

For $\mathbf{x} \in F^I$ let ${}^n\mathbf{x} \in F^n$ with ${}^n\mathbf{x}(i) = \begin{cases} x_i & \text{for } i \in I \\ 0 & \text{for } i \in I' \end{cases}$. Then $\begin{cases} F^I & \rightarrow F^n \\ \mathbf{x} & \mapsto {}^n\mathbf{x} \end{cases}$ is an embedding and $F^n = {}^n p_I(F^n) \oplus {}^n p_{I'}(F^n)$ is a direct sum. For $\mathbf{w} \in F^n$ we have $\mathbf{w} = {}^n p_I(\mathbf{w}) + {}^n p_{I'}(\mathbf{w})$.

Now, for I an information set for C , let

$$\lambda := (p_I|_C)^{-1} : F^I \rightarrow C \quad \text{and} \quad \gamma_I := \lambda p_I : F^I \rightarrow C.$$

Lemma 1. For $\mathbf{w} \in F^n$ we have: $\mathbf{w} \in C$ if and only if $p_{I'} \gamma_I(\mathbf{w}) = p_{I'}(\mathbf{w})$.

Proof. For $\mathbf{w} \in F^n$, $\lambda p_I(\mathbf{w}) = \mathbf{c} \in C$. Hence

$$\mathbf{c} = {}^n p_I \lambda p_I(\mathbf{w}) + {}^n p_{I'} \lambda p_I(\mathbf{w}) = {}^n p_I(\mathbf{w}) + {}^n p_{I'} \lambda p_I(\mathbf{w}) = \mathbf{w}$$

if and only if $p_{I'}(\mathbf{w}) = p_{I'} \lambda p_I(\mathbf{w})$. \square

For an information set I

$$\text{syn}_I : \begin{cases} F^n & \rightarrow F^{I'} \\ \mathbf{w} & \mapsto p_{I'}(\mathbf{w}) - p_{I'} \gamma_I(\mathbf{w}) \end{cases}$$

is by Lemma 1 a check mapping. For $\mathbf{w} \in F^n$ the image $\text{syn}_I(\mathbf{w})$ is called the *syndrome* of \mathbf{w} (with respect to I).

¹ For the definition see [2], p. 1350.

Theorem 1. Let $C \subset F^n$ be a t -error-correcting linear $[n, k, d]$ -code and I an information set for C . For $\mathbf{w} \in F^n$, $\mathbf{c} \in C$ and $\mathbf{e} := \mathbf{w} - \mathbf{c}$ we have:

- (1) $p_I(\mathbf{e}) = \mathbf{0} \iff \mathbf{c} = \gamma_I(\mathbf{w})$
- (2) $p_I(\mathbf{e}) = \mathbf{0} \implies \text{wt}(\text{syn}_I(\mathbf{w})) = \text{wt}(\mathbf{e})$
- (3) $p_I(\mathbf{e}) \neq \mathbf{0}$, $\text{wt}(\mathbf{e}) \leq t \implies \text{wt}(\text{syn}_I(\mathbf{w})) > t$
- (4) If $\text{wt}(\mathbf{e}) \leq t$ then: $p_I(\mathbf{e}) = \mathbf{0} \iff \text{wt}(\text{syn}_I(\mathbf{w})) \leq t$.

Proof. (1) $\gamma_I(\mathbf{w}) = \gamma_I(\mathbf{c}) + \gamma_I(\mathbf{e}) = \mathbf{c} + \lambda p_I(\mathbf{e}) = \mathbf{c} \iff p_I(\mathbf{e}) = \mathbf{0}$.

(2) $\text{syn}_I(\mathbf{w}) = \text{syn}_I(\mathbf{e}) = p_{I'}(\mathbf{e}) - p_{I'}(\lambda p_I(\mathbf{e})) = p_{I'}(\mathbf{e})$ and $\text{wt}(\mathbf{e}) = \text{wt}(p_{I'}(\mathbf{e}))$, hence $\text{wt}(\text{syn}_I(\mathbf{w})) = \text{wt}(p_{I'}(\mathbf{e})) = \text{wt}(\mathbf{e})$.

(3) For $\mathbf{x} := \gamma_I(\mathbf{e}) \in C \setminus \{\mathbf{0}\}$ we have $\mathbf{x} = {}^n p_I(\mathbf{e}) + {}^n p_{I'} \lambda p_I(\mathbf{e})$ by Lemma 1.

Hence

$$\begin{aligned} \text{wt}(\text{syn}_I(\mathbf{w})) &= \text{wt}(\text{syn}_I(\mathbf{e})) = \text{wt}(p_{I'}(\mathbf{e}) - p_{I'}(\mathbf{x})) \geq \text{wt}(-p_{I'}(\mathbf{x})) - \text{wt}(p_{I'}(\mathbf{e})) \\ &= \text{wt}(p_{I'} \lambda p_I(\mathbf{e})) + \text{wt}(p_I(\mathbf{e})) - \text{wt}(p_I(\mathbf{e})) - \text{wt}(p_{I'}(\mathbf{e})) = \text{wt}(\mathbf{x}) - \text{wt}(\mathbf{e}) \\ &\geq d - t \geq 2t + 1 - t \geq t + 1. \end{aligned}$$

(4) follows from (2) and (3). \square

Let $C \subset F^n$ be a t -error-correcting linear $[n, k, d]$ -code and let I be an information set for C . A subset $\Sigma \subset \text{Aut } C$ is called a *permutation decoding set*, shortly *PD-set*, if for every subset $B \subset \{1, \dots, n\}$ with $|B| \leq t$ there exists an automorphism $\alpha \in \Sigma$ with permutation part σ_α such that $\sigma_\alpha(B) \cap I = \emptyset$ or equivalently $B \cap \sigma_\alpha^{-1}(I) = \emptyset$ (cf. [2], p. 1413).

From Theorem 1 follows (cf. [2]) the

Permutation decoding algorithm:

Let $\Sigma = \{\alpha_1, \dots, \alpha_l\}$ be a t -PD-set for the linear code C .

1. For a received senseword $\mathbf{w} \in F^n$ compute $\alpha_i(\mathbf{w})$, $\gamma_I(\alpha_i(\mathbf{w}))$ and $\text{wt}(\text{syn}_I \alpha_i(\mathbf{w}))$ for $i = 1, 2, \dots$ until j is found with $\text{wt}(\text{syn}_I \alpha_j(\mathbf{w})) \leq t$.
2. Compute $\alpha_j^{-1}(\gamma_I(\alpha_j(\mathbf{w})))$.
3. \mathbf{w} is decoded to $\mathbf{c} := \alpha_j^{-1}(\gamma_I(\alpha_j(\mathbf{w}))) \in C$.
4. If $\text{wt}(\text{syn}_I \alpha_1(\mathbf{w})), \dots, \text{wt}(\text{syn}_I \alpha_l(\mathbf{w})) > t$ then there is no $\mathbf{c} \in C$ with $\varrho(\mathbf{w}, \mathbf{c}) \leq t$.

3. Antiblocking decoding

Let P be a finite set. Let \mathfrak{A} be a subset of the powerset 2^P of P . The elements of P and \mathfrak{A} are called *points* and *blocks* respectively. \mathfrak{A} is called a t -antiblocking system of P if

AB For every $B \subset P$ with $|B| = t$ there exists an $A \in \mathfrak{A}$ such that $A \cap B = \emptyset$

holds, and if any two blocks $A, A' \in \mathfrak{A}$ have the same cardinality $|A| = |A'|$. Further, if all blocks have the same cardinality k , then we say the t -antiblocking system \mathfrak{A} has *order* k .

Let $C \subset F^n$ be a t -error-correcting linear $[n, k, d]$ -code and let I be an information set for C .

For every $\alpha \in \text{Aut } C$ the set $\sigma_\alpha^{-1}(I)$ is an information set for C .

Let Σ be a PD-set. Then $\mathfrak{A} := \{\sigma_\alpha^{-1}(I) \mid \alpha \in \Sigma\}$ is a t -antiblocking system of $P_n := \{1, \dots, n\}$ with the property that every block $A \in \mathfrak{A}$ is an information set.

Let \mathfrak{A} be a t -antiblocking system. \mathfrak{A} is called an *antiblocking information system* for C , for short *t-AI-system* for C , if every block $A \in \mathfrak{A}$ is an information set for C .

As already mentioned in the introduction the set \mathcal{I} of all information sets for C is a t -AI-system. That is, for any t -error-correcting linear code there exists a t -AI-system.

Lemma 2. Let \mathfrak{A} be a t -AI-system for the linear code C . For $\mathbf{w} \in F^n$ and $\mathbf{c} \in C$, $\mathbf{e} := \mathbf{w} - \mathbf{c}$ with $\text{wt}(\mathbf{e}) \leq t$ there exists an $A \in \mathfrak{A}$ with $\text{wt}(\text{syn}_A(\mathbf{w})) \leq t$ and $\mathbf{c} = \gamma_A(\mathbf{w})$.

Proof. Let $B := \text{supp}(\mathbf{e})$. By assumption $|B| \leq t$. Hence there exists an $A \in \mathfrak{A}$ with $A \cap B = \emptyset$. Then $p_A(\mathbf{e}) = \mathbf{0}$, and thus $\text{wt}(\text{syn}_A(\mathbf{w})) \leq t$ and $\mathbf{c} = \gamma_A(\mathbf{w})$ by Theorem 1. \square

From Lemma 2 and Theorem 1 follows the

Antiblocking decoding algorithm: Let \mathfrak{A} be a t -AI-system for the linear $[n, k, d]$ -code C .

1. For a received senseword $\mathbf{w} \in F^n$ compute $\gamma_A(\mathbf{w})$ and $\text{wt}(\text{syn}_A(\mathbf{w}))$ for $A \in \mathfrak{A}$ until an A' is found with $\text{wt}(\text{syn}_{A'}(\mathbf{w})) \leq t$.
2. \mathbf{w} is decoded as $\mathbf{c} = \gamma_{A'}(\mathbf{w}) \in C$.
3. If $\text{wt}(\text{syn}_A(\mathbf{w})) > t$ for all $A \in \mathfrak{A}$ then there does not exist a $\mathbf{c} \in C$ with $\varrho(\mathbf{w}, \mathbf{c}) \leq t$.

As the permutation decoding algorithm is more effective the smaller the t -PD-set Σ , also the antiblocking decoding algorithm is more effective the smaller the t -AI-system \mathfrak{A} . By the Theorem of Gordon [1] for any t -PD-set Σ and any t -AI-system \mathfrak{A} of a t -error-correcting linear $[n, k, d]$ -code the following inequalities hold (cf. also [5]):

$$|\Sigma| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil$$

$$|\mathfrak{A}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil.$$

The number $\left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil$ is called the *Gordon bound*.

Let $I, I' \in \mathcal{I}$ be two information sets of the code C . I and I' are called *isomorphic* if there exists an automorphism α of C with $I = \sigma_\alpha(I')$. If Σ is a t -PD-set then the corresponding t -AI-system $\mathfrak{A}(\Sigma) = \{\sigma_\alpha^{-1}(I) \mid \alpha \in \Sigma\}$ belongs to the isomorphism class of the information set I . If we however look for a t -AI-system we are not restricted to look only for information sets belonging to one fixed isomorphism class and so it can be easier to find a small t -AI-system than a small t -PD-set.

Example. In [4] we presented a 5-PD-set Σ_1 for the $[25, 4, 16]$ -code C related to a hyperbolic quadric in $\text{PG}(3, 4)$ with $|\Sigma_1| = 12$ (cf. [4], Proposition 10). Let $\bar{K} := \text{GF}(4) \cup \{\infty\}$, $d \in K$ with $d^2 = d + 1$ and $P := \bar{K} \times \bar{K}$. Here the set P_{25} of the coordinate indices corresponds to P .

Note, an information set for a code defined by a projective system corresponds to a base contained in the projective system.

Let $A = \{(x_i, y_i) \in P \mid i = 1, 2, 3, 4\}$. If there exist i, j, k, l with $\{i, j, k, l\} = \{1, 2, 3, 4\}$ such that $x_i = x_j \neq x_k$, $y_i \neq y_j$ and $x_k = x_l$, $y_k \neq y_l$ or if $y_i = y_j \neq y_k$, $x_i \neq x_j$ and $y_k = y_l$, $x_k \neq x_l$, i.e., the four points lie on two generators of the same kind, then A is an information set for C .

$$\begin{aligned} \text{Let } A_0 &= \{(0, 0), (1, 0), (0, 1), (1, 1)\}, & A_1 &= \{(0, d), (1, d), (0, d+1), (1, d+1)\}, \\ A_2 &= \{(d, 1), (d+1, 1), (d, d), (d+1, d)\}, & A_3 &= \{(d, d+1), (d+1, d+1), (d+1, \infty), (\infty, \infty)\}, \\ A_4 &= \{(0, \infty), (1, \infty), (d+1, 0), (\infty, 0)\}, & A_5 &= \{(d, 0), (d, \infty), (\infty, 1), (\infty, d)\}. \end{aligned}$$

Then $\mathfrak{A} := \{A_0, A_1, A_2, A_3, A_4, A_5\}$ is a 5-AI-system. The Gordon bound is 6.

Jennifer D. Key informed us that she looked at the codes from the desarguesian affine planes of orders $p = 5, 7$ and 11 , using the collection of information sets as a universe from [3] and that she found

- 2-AI-systems of size 15 for $p = 5$ (Gordon bound is 8) whereas the best she got for a 2-PD-set was size 18,
- 2-AI-systems of size 19 for $p = 7$ (Gordon bound is 7) whereas the best she got for a 2-PD-set was size 23,
- 2-AI-systems of size 24 for $p = 11$ (Gordon bound is 4) whereas the best she got for a 2-PD-set was size 26.

Acknowledgement

We would like to thank Professor Jennifer Key for her fruitful suggestions and information that improved our manuscript.

References

- [1] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, *IEEE Trans. Inform. Theory* 28 (1982) 541–543.
- [2] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998, pp. 1345–1440 (Chapter 17).
- [3] J.D. Key, T.P. McDonough, V.C. Mavron, Information sets and partial permutation decoding for codes from finite geometries, *Finite Fields Appl.* 12 (2006) 232–247.
- [4] H.-J. Kroll, R. Vincenti, PD-sets for the codes related to some classical varieties, *Discrete Math.* 301 (2005) 89–105.
- [5] H.-J. Kroll, R. Vincenti, Antiblocking systems and PD-sets, *Discrete Math.* 308 (2008) 408–414.
- [6] F.J. MacWilliams, Permutation decoding of systematic codes, *Bell System Tech. J.* 43 (1964) 485–505.
- [7] E. Prange, The use of information sets in decoding cyclic codes, *IRE Trans. Inform. Theory* 8S (1962) S5–S9.