D.5.2.

Decoding of Superimposed Codes in Multiaccess Communication

Peter de Laval, Shakir Abdul-Jabbar
Department of Electrical Engineering
Linköping University, Sweden

Abstract

Ways of sharing a common channel without feedback are considered. The channel is assumed to be a multiaccess OR channel and the decoding problem is considered for a certain class of superimposed codes. A decoding algorithm is proposed and analysed in terms of maximal decoding complexity. The robustness of the decoding algorithm is tested by simulations of decoding beyond the designed capability of the code.

1. Introduction

The structure of "computer to computer"-traffic is often referred to as "bursty". With this we mean that the peak to average ratio of the traffic load is very high. To use fixed channel assignments in these situations is a big waste, since most of the channel will either be left idle or there will be very large delays for the message transmissions. For bursty traffic situations it is common to share the channel by demand control. The most popular way to share the channels on demand are based on "random time division multiple access" (RTDMA) like Aloha, CSMA or splitting Algorithms. All RTDMA algorithms utilize feedback from the channel. It is essential that the feedback information is reliable and instantaneous, otherwise most of these access algorithms perform poorly.

In many situations it is hard to get reliable and instantaneous feedback, but it is still desirable to share the channel upon demand. In these cases *superimposed codes* can be used to allow more than one user to use the channel in every moment.

In section 2 of this paper the basic concepts of superimposed codes and the channel model are described. The main topic of this paper is the decoding problem. The decoder performs a mapping from a binary sequence into a set of codewords. This problem is quite different from the well known problem of decoding an error correcting code. In section 3 two decoding algorithms are presented. In section 4 some tests of the robustness of the decoders are described.

2. Basic Concepts

Definition *Correlation*

The *correlation*, denoted $c(\mathbf{x},\mathbf{y})$, of two binary sequences $\mathbf{x}$ and $\mathbf{y}$ of length n is defined as

$$c(\mathbf{x},\mathbf{y}) \triangleq \sum_{i=1}^{n} x_i \cdot y_i \quad ,$$

where x_i and y_i are the i:th binary symbols of $\mathbf{x}$ and $\mathbf{y}$ respectively.

Definition *Superposition of binary sequences*

The *superposition* $\mathbf{x} \vee \mathbf{y}$ of two binary sequences $\mathbf{x}$ and $\mathbf{y}$ of length n is defined as

$$\mathbf{x} \vee \mathbf{y} \triangleq \mathbf{z} = (z_1, z_2, \ldots, z_n)$$

where $$z_i \triangleq \begin{cases} 0 & \text{if } x_i = y_i = 0 \\ 1 & \text{otherwise} \end{cases} .$$

The superposition of a set $A = \{ \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)} \}$ of n-dimensional binary sequences is denoted by

$$f(A) \triangleq \mathbf{x}^{(1)} \vee \mathbf{x}^{(2)} \vee \ldots \vee \mathbf{x}^{(m)}.$$

Definition *Multiaccess OR Channel*

With a *multiaccess OR channel* we mean a channel that operates on a set A of binary sequences and produces an output sequence $\mathbf{z}$ equal to the superposition of the input set, i.e.

$$\mathbf{z} \triangleq f(A) .$$

This definition implies that the users are block and bit synchronized.

Definition *Disjunctive Code*

The binary code C with codeword length n and size T is a *disjunctive code* (also called *zero false dropping code*) of order m if each subset $A \subseteq C$ of size $|A| \leq m$ has the property that for every word $\mathbf{x} \in A$ we have $c(\mathbf{x},f(A)) = w_H(\mathbf{x})$ but for all other words $\tilde{\mathbf{x}} \in C \backslash A$ we have $c(\tilde{\mathbf{x}},f(A)) < w_H(\tilde{\mathbf{x}})$. The set of all disjunctive codes with parameters n, m and T is denoted $\mathcal{D}($ n,m,T).

The class of *superimposed codes* consists of the class of *disjunctive codes* and the class of *uniquely decipherable*

88CH2607-0 C 1988 IEEE

codes. The uniquely decipherable codes are very closely related to the disjunctive codes and might in some sense be an easier concept to understand. In spite of this have we chosen to only use the properties of disjunctive codes in this paper since this class have stronger properties. All these concepts were introduced by W.H. Kautz and R.C. Singleton [1].

From the definition of disjunctive codes we see that this class of codes can be used to solve the access problem for a multiaccess OR channel. We know that it is possible to decode any set A of input codewords sent over the channel by observing the output sequence as long as the cardinality of A is smaller than or equal to m.

Definition *Constant Weight Code*

The binary code C with codeword length n and size $|C| = T$ is a *constant weight code* (shortened CW code) if all codewords $\mathbf{x} \in C$ have the same Hamming weight $w_H(\mathbf{x}) = w$. One interesting parameter for the constant weight codes is the *maximum correlation* c. The maximum correlation is defined as

$$c \triangleq \max_{\mathbf{x} \neq \mathbf{y}} c(\mathbf{x},\mathbf{y}) \quad ; \mathbf{x},\mathbf{y} \in C$$

and is related to the minimum distance d by the identity

$$d = 2 \cdot w - 2 \cdot c \ .$$

The set of all constant weight codes with parameters n, w, c and T is denoted $\mathcal{CW}($ n,w,c,T $)$.

Relation between CW codes and disjunctive codes

$$\mathcal{CW}(\text{ n,w,c,T }) \subseteq \mathcal{D}(\text{ n,m}= \lceil w / c \rceil - 1\text{,T}) \qquad (1)$$

where $\lceil a \rceil$ means "smallest integer larger than or equal to a". Proof can be found in [2].

Definition *KS Code*

With a *KS code* we mean a constant weight code constructed by concatenation(see [3]). The outer code is a Reed-Solomon code (RS code) over GF(q) and the inner code is an orthogonal weight one code (i.e. an element of the set $\mathcal{CW}$(n=q,w=1,c=0,T=q)).

The abbreviation KS stands for Kautz-Singleton. This code construction was first proposed by W.H. Kautz and R.S. Singleton in their paper [1] from 1964.

Without loss of generality we will define the inner $\mathcal{CW}$(q,1,0,q) code by the following mapping from symbols from GF(q) to q-dimensional binary vectors :

$$0 \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, 1 \rightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, q-1 \rightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \qquad (2)$$

If $\mathbf{c}_{RS}$ is a codeword from an RS code over GF(q), then with $F(\mathbf{c}_{RS})$ we mean the transformation from the RS codeword into a KS codeword by the mapping given in (2) for each of the symbols of the RS codeword.

Lemma

For all sets of integers w, c and q obeying condition i) and ii) below, there exists a KS code. These KS codes will be elements of the set $\mathcal{CW}(n=w \cdot q,w,c,T=q^{c+1})$.

i) $q = p^s$, where p is a prime and s is any positive integer.
ii) $0 \leq c < w \leq q + 1$

For proof see reference [4]

Definition $\mathcal{KS}$(q,w,c) , *Designed Order*

With $\mathcal{KS}$(q,w,c) we mean the set of KS codes with parameters q, w and c. The integer $m_d = \lceil w / c \rceil - 1$ is referred to as the *designed order* of the KS code.

From the relations (1) we know that we can construct disjunctive codes from CW codes. The KS code construction is one way to get CW codes. It turned out that among the class of KS codes there are disjunctive codes with a relatively short codeword length n for a given code size T and designed order m_d. These results can be found in [2]. It also turned out that the nice and simple structure of the KS codes makes the decoding problem easier to solve.

3. Decoding Algorithms

With a *decoder for superimposed codes* we mean the mapping from the binary superimposed sequence $f(A)$ formed by a multiaccess OR channel into a set of codewords from a given superimposed code C. Let $\hat{A}$ denote the decoder output set. If the decoded set $\hat{A}$ equals the transmitted set A we say that the *decoding was successful*.

Decoding Algorithm 1 *Exhaustive Search*

Let C be a disjunctive code. The *exhaustive search* decoder operates on the received sequence $f(A)$ and outputs a set of codewords $\hat{A}$. $\hat{A}$ is called the decoded set and is defined by

$$\hat{A} \triangleq \{ \mathbf{x} \in C \ | \ c(\mathbf{x},f(A)) = w_H(\mathbf{x}) \} .$$

It is easy to see that this mapping will always lead to a successful decoding as long as the size of the set A is less than or equal to the order of the disjunctive code (this follows from the definition of disjunctive codes). The algorithm has to correlate every codeword $\mathbf{x} \in C$ to the received sequence $f(A)$, i.e. the decoder has to perform exactly T comparisons. We will soon present "better" decoding algorithms, but first we must define some kind of measurement of how good an algorithm is.

Definition *Decoding Complexity*

Let $B(f(A)) \subseteq C$ be the set of codewords that a decoding algorithm D has specified as an intermediate step in the decoding of the received sequence $f(A)$. It is among the codewords in the set $B(f(A))$ that decoder D looks for the codewords to form the decoded set $\hat{A}$. The decoder chooses the codewords to form $\hat{A}$ by correlating each of the elements in $B(\mathrm{f}(A))$ to the received sequence $\mathrm{f}(A)$, or formally written

$$\hat{A} \triangleq \{ \mathbf{x} \in B(\mathrm{f}(A)) \mid \mathrm{c}(\mathbf{x},\mathrm{f}(A)) = \mathrm{w_H}(\mathbf{x}) \}.$$

With *Decoding Complexity* $DC(\mathrm{f}(A))$ of decoder D and received sequence $\mathrm{f}(A)$ we mean the size of the set $B(\mathrm{f}(A))$. With *Maximal Decoding Complexity* $MDC(\mathrm{m_0})$ of decoder D and order $\mathrm{m_0}$ we mean

$$MDC(\mathrm{m_0}) \triangleq \max \; |B(\mathrm{f}(A))| \text{ such that } |A| = \mathrm{m_0}.$$

These complexity measurements are quite rough, but will anyway give some indication of which algorithm is to be preferred to other algorithms. The measurements can be used since the suggested algorithms in this paper all use correlation between codewords and received sequence as one major step in the decoding.

The exhaustive search decoder has decoding complexity independent of the transmitted set of codewords and

$$MDC(\mathrm{m_0}) = DC(\mathrm{f}(A)) = \mathrm{T} \qquad \forall A \subseteq C.$$

The main algorithm of this paper is the next decoder algorithm to be described. This algorithm works only for KS codes and it utilizes the structure from the RS code and the fact that it is easy to find the "transmitted" elements from GF(q) in the received sequence. To make things clearer we give a simple example.

Example

Let $\mathrm{G_{RS}}$ be the generator matrix for an RS code over GF(7) that together with the inner code mapping (2) defines a KS code C_{KS}. We choose

$$\mathrm{G_{RS}} = \begin{pmatrix} 1\,0\,6\,5\,4\,3 \\ 0\,1\,2\,3\,4\,5 \end{pmatrix}.$$

$$C_{\mathrm{KS}} \in \mathcal{KS}(\mathrm{q{=}7,w{=}6,c{=}1}) \subseteq \mathcal{CW}(\mathrm{n{=}42,w{=}6,c{=}1,T{=}49}) \subseteq \subseteq \mathcal{D}(\mathrm{n{=}42,m{=}5,T{=}49}).$$

By multiplying the generator matrix with a information vector **i** of two GF(7)-symbols, we get the RS codeword $\mathbf{c}^{\mathbf{i}}_{\mathrm{RS}}$ .If for instants **i** = (1 3), we get

$$\mathbf{c}^{1,3}_{\mathrm{RS}} = \mathrm{G_{RS}} \cdot (1 \;\; 3) = (1 \;\; 3 \;\; 5 \;\; 0 \;\; 1 \;\; 4).$$

This RS codeword can now be transformed into a KS codeword $\mathbf{c}^{1,3}_{\mathrm{KS}}$,

$$\mathbf{c}^{1,3}_{\mathrm{KS}} = \mathrm{F}(\mathbf{c}^{1,3}_{\mathrm{RS}}) = \begin{pmatrix} 0&0&0&1&0&0 \\ 1&0&0&0&1&0 \\ 0&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&1&0&0&0 \\ 0&0&0&0&0&0 \end{pmatrix}.$$

Each user has such a codeword matrix. Now let A be the set of three codewords from three different users. We will see what happens if they use the multiaccess OR channel simultaneously. Assume that $A = \{ \mathbf{c}^{1,1}_{\mathrm{KS}}, \mathbf{c}^{1,3}_{\mathrm{KS}}, \mathbf{c}^{2,4}_{\mathrm{KS}} \}$. The superposition of A is then

$$\mathrm{f}(A) = \begin{pmatrix} 0&0&0&1&0&0 \\ 1&1&1&1&1&1 \\ 1&0&0&0&0&0 \\ 0&1&0&0&1&0 \\ 0&1&0&0&0&1 \\ 0&0&1&0&0&1 \\ 0&0&1&0&0&0 \end{pmatrix}.$$

Here we see that it is easy to find the symbols from GF(7) in each position of the RS codewords. The first position of the RS codewords (i.e. the first column of the superposition) is either one or two. In the second position of the RS codewords we have one, three and four as GF(7) symbols, etc. .

Definition

Let $\mathrm{f}(A)$ be the superposition of a set A of codewords from a code $C \in \mathcal{KS}(\mathrm{q,w,c})$. The binary sequence $\mathrm{f}(A)$ can be written in a matrix form as a q x w binary matrix.

$$\mathrm{f}(A) = \begin{pmatrix} \mathrm{f_{01}} & \mathrm{f_{02}} & \cdots & \mathrm{f_{0w}} \\ \mathrm{f_{11}} & \mathrm{f_{12}} & \cdots & \mathrm{f_{1w}} \\ \vdots & \vdots & & \vdots \\ \mathrm{f_{(q-1)1}} & \mathrm{f_{(q-1)2}} & \cdots & \mathrm{f_{(q-1)w}} \end{pmatrix}, \quad \mathrm{f_{ij}} \in \{0,1\}.$$

Let $S_{\mathrm{j}}(\mathrm{f}(A))$ denote the set of GF(q) symbols defined by the following mapping

$$S_{\mathrm{j}}(\mathrm{f}(A)) \triangleq \{ \mathrm{x} \in \mathrm{GF(q)} \mid \mathrm{f_{xj}} = 1 \} \quad \mathrm{j} = 1, 2, \ldots ,\mathrm{w}.$$

Decoding Algorithm 2 *Reduced Search*

Let $C \in \mathcal{KS}(\mathrm{q,w,c})$ be defined by the generator matrix $\mathrm{G_{RS}}$ of a systematic RS code over GF(q). Let $B(\mathrm{f}(A))$ be a set of codewords from the code C. This set is defined by

$$B(\mathrm{f}(A)) \triangleq \{ \mathrm{F}(\mathrm{G_{RS}} \cdot \mathbf{i}) \mid \mathbf{i} = (\mathrm{i_1}\;\mathrm{i_2} \ldots \mathrm{i_{c+1}}),\; \mathrm{i_j} \in S_{\mathrm{j}}(\mathrm{f}(A)) \}.$$

The *Reduced Search* decoding algorithm is then defined by

$$\hat{A} \triangleq \{ \mathbf{x} \in B(\mathrm{f}(A)) \mid \mathrm{c}(\mathbf{x},\mathrm{f}(A)) = \mathrm{w} \}.$$

The decoding complexity of the reduced search decoder is equal to

$$DC(\mathrm{f}(A)) = |S_1(\mathrm{f}(A))| \cdot |S_2(\mathrm{f}(A))| \cdot \ldots \cdot |S_{\mathrm{c+1}}(\mathrm{f}(A))|.$$

Thus the $MDC(\mathrm{m_0})$ is equal to $\mathrm{m_0}^{(\mathrm{c+1})}$. It is easy to show that the decoded sets from the reduced search algorithm and the exhaustive search algorithm will always be equal.

Example continuation.

The set $S_1(\mathrm{f}(A))$ is equal to { 1,2 } and the set $S_2(\mathrm{f}(A))$ is equal to { 1,3,4 }. $B(\mathrm{f}(A))$ will then be

$$B(\mathrm{f}(A)) = \{ \mathrm{F}(\mathbf{c}^{1,1}_{\mathrm{RS}}), \mathrm{F}(\mathbf{c}^{1,3}_{\mathrm{RS}}), \mathrm{F}(\mathbf{c}^{1,4}_{\mathrm{RS}}), \mathrm{F}(\mathbf{c}^{2,1}_{\mathrm{RS}}), \mathrm{F}(\mathbf{c}^{2,3}_{\mathrm{RS}}), \mathrm{F}(\mathbf{c}^{2,4}_{\mathrm{RS}}) \}.$$

The decoding complexity $DC(\mathrm{f}(A))$ is equal to 6, and the maximal decoding complexity MDC(3) is equal to 9. If we correlate the six codewords of the set $B(\mathrm{f}(A))$ to the superposition $\mathrm{f}(A)$ we find that three of these correlate up to the weight w of the codewords. These three codewords are the ones chosen by the reduced search decoder and they are also equal to the transmitted set A. With an

$\lvert A\rvert$	Size of decoded set $\hat{A}$ $\lvert A\rvert$	$\lvert A\rvert+1$	$\lvert A\rvert+2$	*MDC*	Average *DC*
6	<1	>0		216	156.2
7	0.999	0.001		343	232.9
8	0.995	0.005		512	325.4
9	0.981	0.019	>0	729	437.2
10	0.937	0.061	0.002	1000	558

Table 1. Performance of code C_1 and the reduced search decoder.

exhaustive search decoder we would have to compare f(A) to all of the 49 codewords of the code.

4. Decoding Beyond The Designed Order

If the transmitted set A is larger than the designed order of a KS code used over a multiaccess OR channel, we are not guarantied that the decoding is successful. It is quite simple to show that with the decoding algorithms suggested we will always have the transmitted set A as a subset of the decoded set $\hat{A}$. In many cases it is possible that the decoding is successful even though the size of A is larger than the designed order.

We illustrate decoding beyond the designed order by some examples. The reduced search decoder has been tested for two different KS codes by computer simulations. Both codes have designed order m_d equal to five, comparable codeword length n≈250 and a code size larger than 10^4. Code C_1 is an element of $\mathcal{KS}(23,11,2)$, code C_2 is an element of $\mathcal{KS}(16,16,3)$. Below follows a list of the codes expressed as CW codes :

$$C_1 \in \mathcal{CW}(253,11,2,12167)$$
$$C_2 \in \mathcal{CW}(256,16,3,65536)$$

The reduced search decoder and the code C_1 will lead to an $MDC(m_0)$ equal to m_0^3, while the $MDC(m_0)$ for code C_2 equals m_0^4.

In table 1 - 2 we will give the results from the simulations for the three given codes. The simulations uses a random generator to pick the set A. The superposition of this set is fed to the reduced search decoder. We let the size of A vary from six up to ten. If the decoded set $\hat{A}$ has the same size as the transmitted set A we know that they are equal and that the decoding was successful. If the decoded set differed from the transmitted set we know that the decoded set will be the larger one. In the tables we give the relative frequency of the size of the decoded set for a given size of the transmitted set. We also give the *MDC* and average *DC* for each size of the set A. When ">0" is found in the tables it means that we know that the decoder gives sets of this size as an output for certain transmitted sets, but that the occurrence of that event is not well estimated by the limited number of different transmitted sets tested (like in table 1 for $\lvert A\rvert=6$ we found 2 subsets out of 20 000 tested that gave $\lvert\hat{A}\rvert=7$). The blank parts of the tables indicate events that did not occur during the simulations, but we do not claim that these events are impossible.

We can see that code C_1 is superior to code C_2 in both decoding robustness and decoding complexity, but code C_2 is larger and can therefore offer a larger populations of users.

In many systems it is essential to be sure that all decoded codewords are correct. For these systems we must make sure that the maximal number of simultaneous users does not exceed the designed order m_d of the code chosen.

In other situations it could be accepted that a few extra codewords are added to the transmitted information. Consider a system where the users uses a multiaccess OR channel to make reservations for another channel, the data channel. A centralized station detects and decodes the information on the multiaccess OR channel. This centralized station can make a fare and effective division of the channel capacity by dividing the data channel among the requesting stations. In such reservation system it is not so harmful if the centralized station assigns some channel capacity to some idle stations, as long as it happens very seldom.

Conclusion

The reduced search decoding algorithm has proven to give good decoding capability for a reasonable decoding complexity. The decoding algorithm has performed very well for situations with larger transmission sets than designed order.

References

[1] W.H. Kautz and R.C. Singleton, "Nonrandom Binary Superimposed Codes", IEEE Trans. on Inf. Th., IT-10, No. 4, pp 363-377, 1964.

[2] S. Abdul-Jabbar and P. de Laval, "Constant Weight Codes for Multiaccess Channels without Feedback", EUROCON 88 Conference, Stockholm Sweden, June 1988.

[3] G. D. Forney, Concatenated Codes, M. I. T. Press, Cambridge, MA., 1966.

[4] P. de Laval and S. Abdul-Jabbar, "Decoding of Superimposed Codes", Linköping University, Dept. of EE, Internal Report (to be published)

$\lvert A\rvert$	Size of decoded set $\hat{A}$ $\lvert A\rvert$	$\lvert A\rvert+1$	$\lvert A\rvert+2$	$\lvert A\rvert+3$	$\lvert A\rvert+4$	$\lvert A\rvert+5$	*MDC*	Average *DC*
6	<1	>0					1296	693.9
7	0.998	0.002					2401	1142.7
8	0.981	0.018	>0				4096	1732.7
9	0.919	0.074	0.006	0.001			6561	2462.2
10	0.748	0.204	0.041	0.006	0.001	>0	10000	3358.8

Table 2. Performance of code C_2 and the reduced search decoder.