# Signature Code Design for Fast Fading Channels

Roope Vehkalahti, Tefjol Pllaha and Olav Tirkkonen
Department of Communications and Networking
Aalto University, Finland
Email: {roope.vehkalahti, tefjol pllaha, olav.tirkkonen}@aalto.fi

***Abstract*—We address the problem of codebook design for sparse user detection in fast fading channels, where the fading realization changes from channel use to next. In this scenario, codebook design criteria based on quasi-static fading, and/or channel state information at the receiver, become ineffective. In this paper we suggest new code design principles for signature coding in fast fading channels and provide examples of codes that are built using these methods.**

## I. Introduction

In this paper we consider the problem of synchronous user detection in non-coherent fading channels. In the basic setup we have $N$ users of which a small number will randomly activate and try to indicate to a single receiver that they are active. Typically this is achieved trough signature sequences, where each active user is sending a sequence of $n$ symbols. We assume that these signature sequences are pre-distributed to the users. The number of signatures is larger than the number of orthogonal resources used, which leads to interference when multiple users are simultaneously active.

There exists an extensive literature on design of signature sequences, starting from early work on CDMA and culminating in a rich theory of signature code design principles both in synchronous and asynchronous scenarios [1], [2].

Recently Compressive Sensing inspired multiuser detection algorithms (CS-MUD) for collision resolution of signatures were suggested for example in [3], [4] and [5]. For most recent developments we refer the reader to [6], [7] and [8].

The investigations in the literature are based on assuming quasi-static channels, where each signature will be faded, but the fading stays the same during the transmission of the codeword, and/or on assuming that the channel coefficients are known to the receiver [3], [9].

In practise, for example in mobile communication, the channel under consideration may suffer from time or frequency selective fading, which renders signature code designs based on quasi-static fading unreliable.

In this paper we discuss signature code design for fast fading channels. First we recall why in a quasi-static channel minimizing the *coherence* [10] of the signature code leads to good user detection performance. Then we consider the signature coding problem in the most extreme fast fading case, where each coordinate of the signature sequences faces independent Rayleigh fading. We first show that classical constant amplitude signature sequences do not work well in fast fading channels. Then we introduce a new code design criterion, the *fading coherence*, and provide error probability bounds for codes that are designed by minimizing it, proving an analogue to the quasi-static case.

In the rest of the paper we concentrate on code design for fast fading channels. First we prove a connection between our code design problem and a restricted classical spherical code design problem. We then take advantage of this connection and show how constant weight binary codes can be used as signature codes in fast fading channels. Finally we simulate the constructed codes in fast fading and quasi-static models and see how minimizing fading coherence improves the performance of a code in the fast fading channel.

## II. Channel Model

Throughout the paper we are considering a scenario, where we have a set of users $U$ indexed by $i$ and each of them have an individual signature code vector $\mathbf{x}_i \in \mathbb{C}^n$. We will call this set of vectors $C \subset \mathbb{C}^n$ a signature code designed for $U$ if each element $\mathbf{x}_i \in C$ satisfies $\|\mathbf{x}_i\|^2 = 1$. The number of users $|U| = N \gg n$. We assume that communication happens in a perfectly synchronized manner in blocks of $n$ time units and that the transmission power $r$ is equal for each user.

During a time frame of $n$ units a random set of users $A \subset U$ is trying to indicate to a single receiver that they are active. The combined signal at the receiver then is

$$\mathbf{y}_A = \sum_{i \in A} \sqrt{nr}\ (\mathbf{H}_i \mathbf{x}_i^{\mathrm{T}})^{\mathrm{T}} + \mathbf{v}, \tag{1}$$

where $\mathbf{H}_i \in \mathrm{diag}(\mathrm{M}_n(\mathbb{C}))$ presents fading and $\mathbf{v}$ is a length $n$ i.i.d $\mathcal{CN}(0,1)$ vector representing noise. If all diagonal entries in $\mathbf{H}_i$ are the same, we have quasi-static fading, while if they are statistically independent, we have fast fading. The receiver knows the channel statistics, but does not know the channel realization $\mathbf{H}_i$. After receiving $\mathbf{y}_A$, the receiver tries to detect the set of active users $A$.

For simplicity we consider a scenario where during any time frame there is a maximum of $t$ active users. We assume that the receiver uses a threshold decoder with threshold $s$, which works as follows: If $|\langle \mathbf{y}_A, \mathbf{x}_i \rangle| \geq s$, the receiver declares user $i$ to be active, otherwise user $i$ is declared nonactive.

Given a time frame of $n$ time units and a single user $i$, an error happens when either the decoder declares that user $i$ was not active, while it actually was (missed detection) or when it was detected while it actually was not (false alarm).

Throughout the paper we talk about time units, but obviously the communication can happen also in frequency domain or in both.

## III. Signature Code Design Criteria for Fading Channels

In the following we consider the user detection problem of the previous section and analyze the probabilities of single user missed detection and false alarm in quasi-static and fast fading channels and derive upper bounds for the single user detection error probability $P_e(U,t)$. The resulting bounds will hold for any of the $U$ users as long as at most $t$ of the $U$ users are active at any given time frame. Our bounds will reveal how different channel models leads to different signature code design criteria.

### A. Quasi-Static Channel

Let us now consider quasi-static fading channel, where each signature sequence of an active user fades in an independent way, but the fading is constant during the transmission of the codeword. In the following we will shortly describe how small coherence of the codebook $C$ provides us guarantees for user detection. This analysis is merely presented so that we can contrast it to the fast fading scenario.

We assume that the signature code $C$ satisfies

$$\mu(C) = \max_{i \neq j} \left( \frac{\langle \mathbf{x}_i, \mathbf{x}_j \rangle}{\|\mathbf{x}_i\| \|\mathbf{x}_j\|} \right) = \max_{i \neq j} \langle \mathbf{x}_i, \mathbf{x}_j \rangle \leq \epsilon \ , \tag{2}$$

where $\mu(C)$ is the coherence of the codebook $C$. This is a classical signature code design criterion used already in early works on CDMA communication systems [2] and later in compressed sensing [10].

In the quasi-static fading model, the random matrix $\mathbf{H}_i$ in the general channel model (1) can be replaced by a scalar. If a subset of active users $A \subset U$ is transmitting, the received signal would be

$$\mathbf{y}_A = \sum_{i \in A} \sqrt{nr} \ h_i \ \mathbf{x}_i + \mathbf{v}, \tag{3}$$

where each of the components of the noise vector $\mathbf{v}$ and independent fading coefficients $h_i$ are i.i.d complex Gaussian random variables with zero mean and unit variance.

In order to find the probability for missed detection and false alarm, we have to understand the statistical properties of $|\langle \mathbf{y}_A, \mathbf{x}_i \rangle|^2$.

In [11] we proved that the inner product $\langle \mathbf{y}_A, \mathbf{x}_i \rangle$ is a zero mean Gaussian random variable with variance

$$g = \sum_{x_j \in A} nr |\langle \mathbf{x}_j, \mathbf{x}_i \rangle|^2 + 1. \tag{4}$$

Furthermore we found that if $i \notin A$ then $g \leq 1 + tnr(\epsilon)^2$ and otherwise $g \geq \|\mathbf{x}_i\|^2 nr + 1 = nr + 1$.

By using this result we then proved that given a set of users $U$, threshold $s$, hard activity limit $t$, a signature code $C$, and assuming that $\frac{s}{(nr+1)} < 1$ and $\frac{s}{(n\epsilon^2 tr+1)} > 1$, the probability of error for a single user is upper bounded by

$$P_e(U,t) < \max \left\{ \frac{s\, e^{1-\frac{s}{(nr+1)}}}{nr+1}, \frac{s\, e^{1-\frac{s}{(n\epsilon^2 tr+1)}}}{n\epsilon^2 tr+1} \right\}. \tag{5}$$

In [11] it was also proven that for large values of $r$ (5) can be approximated as

$$P_e(U,t) < \max \left\{ ft\epsilon^2, fe^{1-f} \right\}, \tag{6}$$

where $f > 1$ is a freely chosen parameter. Here we see that the smaller the coherence $\epsilon$ is, the better the bound on error probability becomes.

### B. Fast Fading Channel

Let us now consider a scenario where the single user channels are fast fading. Again we assume a set of user $U$ and corresponding signature code $C$.

If a set of users $A \subset U$ is transmitting the receiver will get

$$\mathbf{y}_A = \sum_{i \in A} \sqrt{nr} (\mathbf{H}_i \mathbf{x}_i^{\mathrm{T}})^{\mathrm{T}} + \mathbf{v}, \tag{7}$$

where each of the $\mathbf{H}_i$ is an independent diagonal $n \times n$ matrix with i.i.d $\mathcal{CN}(0,1)$ random variables on the diagonal and $\mathbf{v}$ is a length $n$ i.i.d $\mathcal{CN}(0,1)$ vector.

Let us consider how signature codes designed for the quasi-static channel would work in this channel model. Assume two users with signature sequences $\mathbf{x}_1 = \frac{1}{\sqrt{2}}(1,1)$ and $\mathbf{x}_2 = \frac{1}{\sqrt{2}}(-1,1)$. For this code $\mu(C) = 0$, and the code is perfect with respect to the coherence. However, after fading, $\mathbf{x}_1$ is $\sqrt{r}(h_{1,1}, h_{1,2})$, while $\mathbf{x}_2$ is $\sqrt{r}(-h_{2,1}, h_{2,2})$. All of the $h_{i,j}$ are identical Gaussian random variables and hence the faded versions of $\mathbf{x}_1$ and $\mathbf{x}_2$ are indistinguishable. It follows that irrespective of the used decoder this code cannot be used in the fast fading channel. On the other hand, if we were to use a signature code with $\mathbf{x}_1 = (1,0)$ and $\mathbf{x}_2 = (0,1)$, it would behave exactly like in the quasi-static channel and we could separate the signals well. Both of the described codes have coherence $0$, but only the second one works in the fast fading channel.

Can we now find a general code design criterion for fast fading channels, that would separate these two codes and would act like coherence does in the quasi-static channel?

**Definition 1.** *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ and define*

$$[\mathbf{x}, \mathbf{y}] := \sqrt{|x_1 y_1|^2 + |x_2 y_2|^2 + \cdots + |x_n y_n|^2}. \tag{8}$$

**Definition 2.** *Let us suppose we have a set of users $U$ and corresponding signature code $C$. We define*

$$\max(C) := \max\{[\mathbf{x}_i, \mathbf{x}_j] \ | \ i,j \in U, i \neq j\},$$

*and call it the* maximum *of $C$.*

Let us now assume that the signature code $C$ satisfies $\max(C) = \epsilon$, and that there exists a hard limit $t$ for the activity.

We then have a result analogous to (4).

**Lemma 1.** *Assume that $A \subset U$, $\mathbf{x}_i \in C$ and $\mathbf{y}_A$ is given by Equation (7). We have that $\langle \mathbf{y}_A, \mathbf{x}_i \rangle$ is a zero mean Gaussian random variable with variance*

$$g = \sum_{j \in A} nr [\mathbf{x}_j, \mathbf{x}_i]^2 + 1. \tag{9}$$

*If $i \notin A$ then $g \leq 1 + tnr(\epsilon)^2$. Otherwise $g \geq [\mathbf{x}_i, \mathbf{x}_i]^2 nr + 1$.*

*Proof.* Additivity of the inner product gives us that

$$\langle \mathbf{y}_A, \mathbf{x}_i \rangle = \sum_{j \in A} \sqrt{nr} \langle (\mathbf{H}_j \mathbf{x}_j^{\mathrm{T}})^{\mathrm{T}}, \mathbf{x}_i \rangle + \langle \mathbf{v}, \mathbf{x}_i \rangle.$$

Equation (9) then follows from the basic properties of Gaussian random variables. The other claims are obtained by analysing the minimization and maximization of (9). □

A comparison of Equations (4) and (9) reveals that in the fast fading channel (8) plays the same role as inner product plays in the quasi-static channel. However, comparing the condition $g \geq [\mathbf{x}_i, \mathbf{x}_i]^2 nr + 1$ from Lemma 1 and $g \geq |\langle \mathbf{x}_i, \mathbf{x}_i \rangle|^2 nr + 1 = nr + 1$ from (4) we can see a difference. While by definition $\langle \mathbf{x}_i, \mathbf{x}_i \rangle$ is always 1 for elements in $C$, $[\mathbf{x}_i, \mathbf{x}_i]$ can have very different values and the bound in Lemma 9 might not be the same for all elements in $C$.

For example we have $[\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,1)] = \frac{1}{\sqrt{2}}$, while $[(1,0),(1,0)] = 1$.

**Definition 3.** *Let $C$ be a signature code. We then define*

$$\min(C) := \min_{\mathbf{x} \in C} \{[\mathbf{x}, \mathbf{x}]\}.$$

Let us now assume that the code $C$ satisfies $\max(C) = \epsilon$, and $\min(C) = \alpha$.

Before proceeding, we need the following result from [12]. Assume that $\chi_k^2$ is a chi-squared random variable with $k$ degrees of freedom. When $0 < z < 1$, we have that

$$p(\chi_k^2 < zk) \leq (ze^{1-z})^{k/2} \tag{10}$$

and for $z > 1$,

$$p(\chi_k^2 > zk) \leq (ze^{1-z})^{k/2}. \tag{11}$$

We then have an analogues result as in (5).

**Proposition 1.** *Given a set of users $U$, threshold $s$, hard activity limit $t$ and a signature code $C$, and assuming that $\frac{s}{(n\alpha^2 r + 1)} < 1$ and $\frac{s}{(n\epsilon^2 tr + 1)} > 1$, we have the following upper bound for the probability of error for a single user*

$$P_e(U,t) < \max\left\{ \frac{s\, e^{1 - \frac{s}{(n\alpha^2 r + 1)}}}{n\alpha^2 r + 1}, \frac{s\, e^{1 - \frac{s}{(n\epsilon^2 tr + 1)}}}{n\epsilon^2 tr + 1} \right\}. \tag{12}$$

*Proof.* Let us first assume that $i \notin A$. The probability for false alarm is

$$p(|\langle \mathbf{y}_A, \mathbf{x}_i \rangle|^2 > s). \tag{13}$$

According to Lemma 1 we know that $\langle \mathbf{y}_A, \mathbf{x}_i \rangle$ is a Gaussian random variable $z'$, with variance $\sigma$. It can be written in an equivalent form $\sqrt{\sigma} z$, where $z$ is complex Gaussian with zero mean and unit variance. Hence we can see that the probability in (13) is maximized when $\langle \mathbf{y}_A, \mathbf{x}_i \rangle$ is the random variable with the largest variance. According to Lemma 1 we have that

$$p\Big(|\langle \mathbf{y}_A, \mathbf{x}_i \rangle|^2 > s\Big) \leq p\Big((1 + tnr\epsilon^2)|z|^2 > s\Big).$$

The final result now follows from (11) as $2|z|^2$ is chi-squared random variable with two degrees of freedom.

In a similar manner, if we assume that user $i \in A$ we have the following upper bound for the probability of missed detection

$$p\Big(|\langle \mathbf{y}_A, \mathbf{x}_i \rangle|^2 \leq s\Big) \leq p\Big((1 + \alpha nr)|z|^2 \leq s\Big).$$

Equation (10), then gives us the final claim. □

For large $r$, (12) can be approximated as

$$P_e < \max\left\{ \frac{(ft\epsilon^2)}{(\alpha^2)}, fe^{1-f} \right\}, \tag{14}$$

where $f > 1$ is a chosen parameter. We can now see that the smaller the value of $\frac{\epsilon}{\alpha}$ is the better the bound is.

**Definition 4.** *Given a signature code $C$, the ratio*

$$d(C) = \frac{\max(C)}{\min(C)} \tag{15}$$

*is the* fading coherence *of the code $C$.*

When comparing (6) and (14) we can see that coherence and fading coherence do play analogous roles in their respective channel models.

A simple signature code design criterion for fast fading channel is thus to find a set of vectors $C \subset \mathbb{C}^n$ where for all $\mathbf{x}_i \in C$, $\|\mathbf{x}_i\| = 1$ and $d(C)$ is as small as possible.

**Example 1.** *Let us consider signature codes $C_1 = \{(0,1),(1,0)\}$ and $C_2 = \{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(-1,1)\}$. We then have $d(C_1) = 0$, but $d(C_2) = 1$, which is in line with our experience that $C_1$ is a good code for fast fading channels and $C_2$ is bad.*

## IV. Signature Codes for Fast Fading Channel

In the previous section we found a code design criterion for signature codes in fast fading channels. We could also see that when $n = N = |C|$ the most simple signature code did work and for such a code $d(C) = 0$. Let us now consider the code design problem when $N > n$. Our goal is to find codes that maximize the number of codewords $|C|$ while keeping $d(C)$ as small as possible. This design problem seems to be quite hard as the definition of the fading coherence $d(C)$ is a quotient of two dependent optimization parameters $\max(C)$ and $\min(C)$, where $\max(C)$ should be minimized while $\min(C)$ should be maximized.

In the code design we can limit ourselves to codebooks where the coordinates of the codewords are non-negative numbers, which we denote with $\mathbb{R}_{x \geq 0}$. This follows as any codebook $C$ can be replaced with another codebook $C'$, where each coordinate of the codewords in $C$ have been replaced by its absolute value. According to Definition 1 we then have that $d(C) = d(C')$ and obviously $|C| = |C'|$. In order to further simplify our problem we will relax the code design criterion and forget the condition that all the codewords of $C$ should have norm 1. With these assumptions for any relevant codebook $C$ we have an other codebook $C^{1/2}$, which is obtained from $C$ by taking a square-root of each of the coordinates of the codewords. With a similar notation, we also have a codebook $C^2$, where each coordinate of the codewords is squared. If we consider a set of codebooks with $N$ codewords and non-negative coordinates, then the mappings $C \mapsto C^{1/2}$ and $C \mapsto C^2$ are bijections.

Given a codebook $C$ we can define

$$m(C) = \frac{\max_{i \neq j} \langle \mathbf{x}_i, \mathbf{x}_j \rangle}{\min_i \|\mathbf{x}_i\|^2} \ . \tag{16}$$

We are interested on this measure as for any codebook $C \subset \mathbb{R}^n_{x \geq 0}$ we have that

$$d(C) = \sqrt{m(C^2)}, \tag{17}$$

which can be seen directly from Definition 1. This reveals that if we find a codebook $C$ with $N$ codewords, which minimizes the value $m(C)$, then the codebook $C' = C^{1/2}$ is the codebook which minimizes the value of $d(C')$ for any $N$ codeword codebook $C'$.

While $m(C)$ is already a more familiar measure than $d(C)$, it is still a quotient of two parameters and finding a codebook minimizing $m(C)$ can be difficult. However, in some cases we can reduce the problem of minimizing $m(C)$ into the simpler problem of minimizing (2).

We say that an $N$ codeword codebook $C$ is *extremal* with respect to $m$ if there does not exist a codebook $C'$ with $N$ codewords satisfying $m(C') < m(C)$. Extremal codebooks with respect to $d$ and $\mu$ are defined similarly.

**Lemma 2.** *Consider an extremal codebook $C$ that minimizes $m(C)$. If the pair of vectors $(a, b) = \arg\max_{i \neq j} \langle \mathbf{x}_i, \mathbf{x}_j \rangle$ gives the extremum of the numerator in* (16)*, this pair also yields the extremum of the denominator: $\|\mathbf{x}_a\| = \|\mathbf{x}_b\| = \min_i \|\mathbf{x}_i\|$.*

*Proof.* We express the vectors in terms of normalized ones as $\mathbf{x}_i = s_i \tilde{\mathbf{x}}_i$, with $\|\tilde{\mathbf{x}}_i\| = 1$. Now

$$m(C) = \frac{\max_{i \neq j} s_i s_j \langle \tilde{\mathbf{x}}_i, \tilde{\mathbf{x}}_j \rangle}{\min_i s_i^2}. \tag{18}$$

Assume the negation of the claim: $s_a > \min_i s_i$ and/or $s_b > \min_i s_i$. By reducing $s_a$ and/or $s_b$ such that we get $s_a = s_b = \min_i s_i$, the denominator in (18) remains the same, but the numerator shrinks, thus $m(C)$ shrinks. This is a contradiction, as the set of vectors was assumed extremal. Accordingly the claim holds. □

We can then prove the following.

**Proposition 2.** *Given an extremal codebook $C$, that minimizes $m(C)$, an equivalent codebook $C'$ exists, for which $\|\mathbf{x}'_i\| = 1$, $\forall\ \mathbf{x}'_i \in C'$, and $\mu(C') = m(C') = m(C)$.*

*Proof.* Assume that $(a, b) = \arg\max_{i \neq j} \langle \mathbf{x}_i, \mathbf{x}_j \rangle$. Again, redefine $\mathbf{x}_i = s_i \tilde{\mathbf{x}}_i$, with $\|\tilde{\mathbf{x}}_i\| = 1$. For all pairs of vectors $\mathbf{x}_i \neq \mathbf{x}_j$ we thus have

$$s_i s_j \langle \mathbf{x}_i, \mathbf{x}_j \rangle \leq s_a s_b \langle \tilde{\mathbf{x}}_a, \tilde{\mathbf{x}}_b \rangle. \tag{19}$$

Also, according to Lemma 1, for all vectors $\mathbf{x}_i$ we have

$$s_i \geq s_a = s_b \ .$$

For any $i \neq a, b$, reduce the scale to be $s'_i = s_a$. This does not change the denominator of $m(C)$. Also $s'_i \leq s_i$. The left-hand side of (19) thus may become smaller, but the numerator of $m(C)$ does not change. Accordingly, all $s_i$ can be chosen equal, $s_i = s$, without changing $m(C)$. After this is done, both the numerator and denominator of $m(C)$ scales as $s^2$. The scale is irrelevant, and can be chosen to be $s = 1$. □

We say that an $N$ codeword codebook $C$ is $\mathbb{R}_{x \geq 0}$*-extremal* with respect to $m$ if there does not exist a codebook $C' \subset \mathbb{R}^n_{x \geq 0}$ with $N$ codewords satisfying $m(C') < m(C)$. Similarly, we define $\mathbb{R}_{x \geq 0}$-extremal codebooks with respect to $d$ and $\mu$.

Given that there exists an $N$ codeword $\mathbb{R}_{x \geq 0}$-extremal code, which minimizes fading coherence $d$ we have the following.

**Corollary 1.** *Let us supppose that $C \subset \mathbb{R}^n_{x \geq 0}$ is an $N$ codeword codebook. Then $C^{1/2}$ is an $N$ codeword codebook and*

$$\sqrt{\mu(C)} = d(C^{1/2}).$$

*If $C$ is $\mathbb{R}_{x \geq 0}$-extremal with respect to $\mu$, then $C^{1/2}$ is extremal with respect to $d$.*

*Proof.* The first result is immediate. Let us now assume that $C$ is extremal with respect to $\mu$. We also assumed that there exists an $N$ codeword $\mathbb{R}_{x \geq 0}$-extremal codebook $C'$, that minimizes $m(C')$. Furthermore, according to Proposition 2 we must have that $m(C') = m(C) = \mu(C)$, or otherwise $C$ would not be $\mathbb{R}_{x \geq 0}$-extremal with respect to coherence. It then follows from (17) that $C^{1/2}$ must be $\mathbb{R}_{x \geq 0}$-extremal with respect to $d$ and $d(C^{1/2}) = \sqrt{\mu(C)}$. □

This result proves that any codebook $C \subset \mathbb{R}^n_{x \geq 0}$ having small $\mu(C)$ provides a good candidate $C^{1/2}$ for the fast fading channel. Furthermore among such codebooks we can find all the extremal codebooks that minimizes the fading coherence.

However, this approach has limitations. It could be that while the codewords of $C$ have all norm 1, the same might not be true for the codewords of $C^{1/2}$. Hence, if we want to have equal power codebooks for the fast fading channel, we can not use this result directly. This argument also suggests that if we like to have maximal separation in the fast fading channel, we might want to use codewords with unequal powers.

### *A. Code Construction From Constant Weight Binary Codes*

In the previous section we saw that codes with non-negative coordinates and small coherence are a promising source of codes for fast fading channels. An example of such codes can be produced from binary codes $G \subset \{0, 1\}^n$.

**Lemma 3.** *Let us suppose we have a constant weight $w$ binary code $G$ with Hamming distance $m$. We then have that $C = \frac{1}{\sqrt{w}} G$ is a signature code where*

$$\mu(C) = \frac{w - \lceil m/2 \rceil}{w} = m(C) \tag{20}$$

*and*

$$d(C) = \frac{\sqrt{w - \lceil m/2 \rceil}}{\sqrt{w}}. \tag{21}$$

*Proof.* Every codeword in $C$ has norm 1. Furthermore, by direct calculation we find that, given two elements $\mathbf{x}_i, \mathbf{x}_j \in C$ with Hamming distance $m$, $\langle \mathbf{x}_i, \mathbf{x}_j \rangle = \frac{w - \lceil m/2 \rceil}{w}$. We can also directly see that $C^2$ is $C$ after normalization. The last equation then follows from (17). $\square$

This result induces a code design problem in the binary domain. In order to minimize (21) we should minimize the cross-correlation of the codewords, just like in the code design for frequency hopping [13] or optical channels [14]. However, the additional division with the weight in (21) does change the problem slightly.

**Example 2.** *A simple length $n$ constant weight code consists of all the weight $w$ binary sequences. The Hamming distance for such codes is always* 2. *According to* (21) *we should use as small weight as possible. With $w = 2$ we can have $\binom{n}{2}$ codewords and $d(C) = \frac{1}{\sqrt{2}}$. A code based on Steiner triple system [15] gives us a length* 25 *code $C_1$ with 100 codewords, weight* 3 *and $d(C_1) = \frac{1}{\sqrt{3}}$.*

The theory of constant weight codes is rich and there exists number of constructions. By considering longer codes we can decrease the value of $d(C)$ and according to (14) support larger number of users. However, compared to the classical coherence, the decay of fading coherence is considerably slower.

## V. Simulations

Our work suggests that minimizing fading coherence of a code leads to good performance in the fast fading channel when using classical matched filter (MF). In the following we will test this hypothesis and simulate the performance of a Steiner system based code $C(25, 3, 2)$ from Example 2 and compare it to a randomly generated code with $\pm 1$ coordinates and 100 codewords. The fading coherence of $C(25, 3, 2)$ is $\frac{1}{\sqrt{3}}$, while the fading coherence of the random code is 1.

In the simulations we assume that the receiver knows that there are exactly $K$ active users. The receiver uses matched filtering and calculates $|\langle \mathbf{y}_A, \mathbf{x}_i \rangle|^2$ for every index $i$. The indices returning the $K$ largest values are considered active. In the fast fading channel we also consider a receiver optimized for fast fading: We first take the absolute value of the coordinates of $\mathbf{y}_A$ and then calculate $|\langle \widetilde{\mathbf{y}}_A, \mathbf{x}_i \rangle|^2$ for the corresponding vector $\widetilde{\mathbf{y}}_A$. We call this Absolute Value Matched Filtering (AV-MF). If $p_k$ denotes the probability for correctly recovering $k$ users, the single user error probability is

$$p_O = 1 - \frac{1}{K} \sum_{i=1}^{k} k \, p_k.$$

When using classical MF decoder the code $C(25, 3, 2)$ performs well in the quasi-static channel, outperforming the random $\pm 1$ code. This can be attributed to the fairly good classical coherence of $C(25, 3, 2)$. In the fast fading channel $C(25, 3, 2)$ provides considerable gain against the random $\pm 1$ code, which could be predicted by the considerable difference in the fading coherences of these codes. When using the AV-MF receiver in the fast fading channel, the performance of $C(25, 3, 2)$ improves considerably.

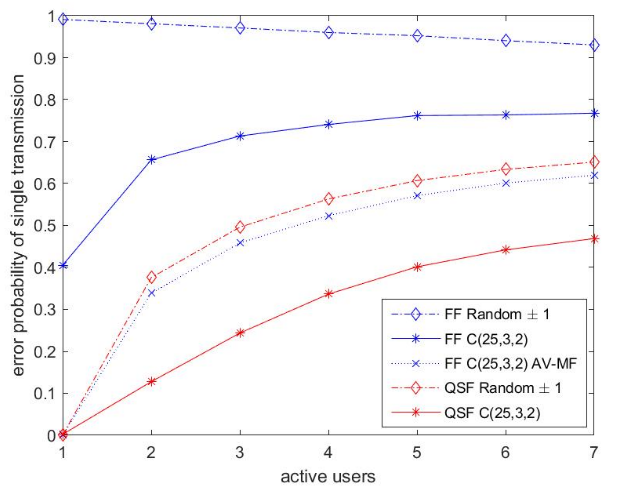


Fig. 1. Comparison of the codes in the quasi-static (QSF) and fast fading (FF) channels with SNR 20 dB

We can now see a trade-off. With the classical MF decoder $C(25, 3, 2)$ performs well in the quasi-static channel, while providing passable performance in the fast fading channel. Thus $C(25, 3, 2)$ can be decoded with the MF in varying channels and without knowing the fading distribution exactly. However, if we know that the channel really is fast fading, we can reap the diversity gain by using the AV-MF receiver. Note that the performance of $C(25, 3, 2)$ could be improved in quasi-static fading by adding phase differences to the codeword coordinates. The benefits of this could be reaped by a conventional MF decoder. If an AV-MF decode were used in quasi-static fading, improvements from phase differences would not be visible.

## VI. Conclusions

In this work we developed a code design criterion for fast fading signature coding. We analyzed the geometric structure of such codes and derived an example code. The code did provide considerable gain in the fast fading channel, when compared to a code with constant amplitude. Furthermore, it did also have reasonable performance in the quasi-static channel. Our approach provides a simple code design criterion, which was proven to work also when we used more specialized receiver.


## Acknowledgements

This work was funded in part by the Academy of Finland (grants 299916 and 319484).

# REFERENCES


[1] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudo-noise and related sequences," *Proc. IEEE*, vol. 68, pp. 598–619, May 1980.

[2] M. Rupf, J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, Vol. 40, pp. 1261–1266 1994.

[3] H. Zhu and G. B. Giannakis, "Exploiting sparse user activity in multiuser detection," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 454–465, Feb. 2011.

[4] H. F. Schepker and A. Dekorsy, "Sparse multi-user detection for cdma transmission using greedy algorithms," 2011 8th *International Symposium on Wireless Communication Systems*, pp. 291–295, Nov. 2011.

[5] L. Applebaum, W. U. Bajwa, M. F. Duarte, and R. Calderbank, "Asynchronous code-division random access using convex optimization," *Physical Communication*, vol. 5, no. 2, pp. 129–147, June 2012.

[6] Z. Chen, F. Sohrabi, and W. Yu, "Sparse activity detection for massive connectivity," *IEEE Trans. Signal Process.*, vol. 66, no. 7, pp. 1890–1904, Apr. 2018.

[7] Z. Utkovski, T. Eftimov, and P. Popovski, "Random access protocols with collision resolution in a noncoherent setting," *IEEE Wireless Commun. Lett.*, vol. 4, pp. 445–448, Aug. 2015.

[8] Y. Ji, C. Stefanovic, C. Bockelmann, A. Dekorsy, and P. Popovski, "Characterization of coded random access with compressive sensing based multi-user detection," in *IEEE GLOBECOM*, pp. 1740–1745, Dec. 2014.

[9] R. Hoshyar, F.P. Wathan, R. Tafazolli, "Novel Low-Density Signature for Synchronous CDMA Systems Over AWGN Channel," *IEEE Trans. Signal Process.*, vol. 56, No. 4, pp. 1616–1626, Apr. 2008.

[10] D. L. Donoho and M. Elad, "Optimally sparse representation in general (nonorthogonal) dictionaries via minimization," *Proc. Nat. Acad. Sci.* USA, vol. 100, no. 5, pp. 2197–2202, 2003.

[11] R. Vehkalahti, T. Pllaha and O. Tirkkonen, "Towards Ultra-Reliable Signature Coding With Multiple Transmit Antennas", to appear in 2021 IEEE 93th Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 2021.

[12] S. Dasgupta and A. Gupta, "An elementary proof of a theorem of Johnson and Lindenstrauss," *Random Structures and Algorithms*, vol. 22, pp. 60–65, 2003.

[13] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming-correlation properties," *IEEE Trans. Inform. Theory*, vol. 20, no. 1, pp. 90–94, Jan. 1974.

[14] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks. I. Fundamental principles," *IEEE Trans. Commun.*, vol. 37, no. 8, pp. 824–833, Aug. 1989.

[15] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, "A new table of constant weight codes", *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.