Multiple Access Euclidean Channel

Danyo DANEV [a] Zoltán FÜREDI [b] Miklós RUSZINKÓ [c]
[a] *Linköping University, Linköping, SWEDEN*
[b] *University of Illinois at Urbana Champaign, and Hungarian Academy of Sciences, Alfréd Rényi Institute of Mathematics*
[c] *Hungarian Academy of Sciences, Computer and Automation Research Institute*

Abstract. Codes for Euclidean Channels are discussed in this chapter. In case of Euclidean Channels the input and output codewords are usually arbitrary members of the n-dimensional Euclidean space $\mathbb{R}^n$. However, by energy constraint reasons the codewords are assumed to have small Euclidean norm: usually they are supposed to have norm one at most. This way they are closely related to spherical codes and "kissing numbers". In addition to this some other constraints are assumed, usually with respect to the Euclidean distance of codewords or groups of codewords. Here we shall discuss the best known bounds and constructions for Multiple Access Euclidean Channels.

Keywords. Euclidean channel, random coding, second moment method.

1. Channel Model

The Euclidean channel is a special case of the multiple-access channel. This channel is an adder channel for real numbers. The channel input and output alphabets are the set $\mathbb{R}$ of real numbers, and the output is simply the sum of the inputs:

$$Y = \sum_{i=1}^{t} X_i.$$

This channel is much like the binary adder channel, the difference is the channel input and output alphabet, which is the set $\mathbb{R}$ of real numbers in the case of the Euclidean channel instead of the set $\{0, 1\}$ and the set $\mathbb{N}$ which is the input and the output alphabet of the binary adder channel, respectively.

We will discuss multiple-access codes for this channel. For simplicity, we use signature codes, where as usual, each user (each component code) has only two elements, and one of these is the all zero. The non-zero one is denoted by $\mathbf{x}^{(i)}$ for the ith user. Let us call users sending their all zero codeword inactive, and users sending their non-zero one as active.

Since the channel is synchronized and deterministic, the channel output is simply the sum of the codewords of the active users. If we denote the set of active users by U, then the channel output is

$$\mathbf{y}_U = \sum_{i \in U} \mathbf{x}^{(i)}.$$

Certainly, if we do not have any noise, then the channel capacity is infinite. To better model real transmissions, we introduce minimal distance and maximal energy constraints. This yields the definition of Euclidean signature codes:

Definition 1. *$\mathcal{C} = \left\{\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(t)}\right\}$ is an Euclidean signature code of length n for t total, and maximum m active users if*

$$\mathbf{x}^{(i)} \in \mathbb{R}^n, \left\|\mathbf{x}^{(i)}\right\| \leq 1 \qquad \forall i \in [t],$$

and

$$d_{min}(\mathcal{C}) \geq d,$$

where

$$d_{min}(\mathcal{C}) = \min_{\substack{U \subseteq [t], V \subseteq [t]: \\ |U| \leq m, |V| \leq m, U \neq V}} \|\mathbf{y}_U - \mathbf{y}_V\|,$$

and $\|.\|$ denotes the Euclidean norm in $\mathbb{R}^n$.

The reason for these constraints is straightforward. Consider some disturbing noise in the communication. The minimum distance criteria makes it possible to recover the messages of the users from the noisy output with a certain fidelity. Certainly, if the codewords are from $\mathbb{R}^n$, the minimum-distance criteria makes no sense without a maximal energy constraint. Codes having properties above are also called in the literature Euclidean superimposed codes as sometimes we will refer to these codes.

Furthermore, we assume, that only a small subset of the users are communicating simultaneously. We will use the m-out-of-t model, where there are t total users out of which at most m are active at any given instant. In our model the minimum distance d is some absolute constant which is independent from the number of codewords t, code length n and maximum active users m.

We also mention here that such codes are often called in the literature spherical superimposed codes and are frequently denoted by (n, d, m, t)-SSC, where n, d, m and t are the above parameters of the code.

For given values of t, m and d, we define the minimal Euclidean signature code length $N_E(t, m, d)$ as the length of the shortest possible Euclidean signature code with this given parameters:

$$N_E(t, m, d) = \min\left\{n \in \mathbb{N}\colon \exists \mathcal{C}(n, t, m) \text{ Euclidean code with } d_{\min}(\mathcal{C}) \geq d\right\}. \qquad (1)$$

Since choosing $U = \{1\}$ and $V = \emptyset$ the distance $\|\mathbf{y}_U - \mathbf{y}_V\| = \left\|\mathbf{x}^{(1)}\right\| \leq 1$, so there are no codes with minimum distance $d_{\min} > 1$, therefore we only consider $N_E(t, m, d)$ for $0 < d \leq 1$.

2. Bounds for Euclidean Signature Codes

It was proved by Ericson and Györfi [1988] using a simple sphere packing argument, that for the minimal Euclidean signature code length defined by (1) the $N_E(t,m,d) \gtrsim \frac{m \log t}{\log m}$ asymptotic lower bound holds. Indeed, this follows from the fact that for *arbitrary* code where the norm of every codeword is at most one the points $\mathbf{y}_U$ $(U \subseteq [t], |U| = m)$ are within a ball of radius of $2\sqrt{m}$.

The main idea of the following improvement is to show that for *arbitrary* code where the norm of every codeword is at most one, say, half of the vectors $\mathbf{y}_U$ $(U \subseteq [t], |U| = m)$ are within a ball of radius of $2\sqrt{m}$. From this, the stronger lower bound on the code length immediately follows by the same sphere packing argument applied to the sphere with radius $2\sqrt{m}$. This proof is an application of the well known "second moment" method.

Theorem 1. *(Füredi–Ruszinkó, [1999])*

$$\liminf_{m\to\infty} \liminf_{t\to\infty} \frac{N_E(t,m,d)\log m}{m \log t} \geq 2,$$

i.e.,

$$N_E(t,m,d) \gtrsim \frac{2m \log t}{\log m}.$$

Notice that this is an exponential improvement for the maximum number of codewords. To prove this theorem, we need the following lemma:

Lemma 1. *For arbitrary code $\mathcal{C} \subseteq \mathbb{R}^n$ ($|\mathcal{C}| = t$) where the norm of every codeword is at most one and arbitrary integer $m << t$ the inequality*

$$\sum_{U\subseteq[t]:\ |U|=m} \|\mathbf{y}_U - m\mathbf{c}\|^2 \leq \binom{t}{m} m$$

holds, where $\mathbf{c} = \frac{1}{t}\sum_{i=1}^{t} \mathbf{x}^{(i)}$ is the average vector.

Proof. We will denote the Euclidean inner product with $\langle ., . \rangle$.

$$\sum_{U\subseteq[t]:\ |U|=m} \|\mathbf{y}_U - m\mathbf{c}\|^2 = \sum_{U\subseteq[t]:\ |U|=m} \left(\|\mathbf{y}_U\|^2 - 2m\langle \mathbf{y}_U, \mathbf{c}\rangle + m^2 \|\mathbf{c}\|^2 \right) \qquad (2)$$

We can do the summation by terms. For the second term,

$$\begin{aligned}
\sum_{U\subseteq[t]:\ |U|=m} -2m\langle \mathbf{y}_U, \mathbf{c}\rangle &= -2m \left\langle \sum_{U\subseteq[t]:\ |U|=m} \mathbf{y}_U, \mathbf{c} \right\rangle \\
&= -2m \binom{t-1}{m-1} t \langle \mathbf{c}, \mathbf{c}\rangle \\
&= -2 \binom{t}{m} m^2 \|\mathbf{c}\|^2,
\end{aligned}$$

since in the sum $\sum_{U\subseteq[t]\colon |U|=m}\mathbf{y}_U$ every vector of code $\mathcal{C}$ is summed up with multiplicity $\binom{t-1}{m-1}$. For the third term,

$$\sum_{U\subseteq[t]\colon |U|=m} m^2\|\mathbf{c}\|^2 = \binom{t}{m} m^2\|\mathbf{c}\|^2.$$

For the first term,

$$\begin{aligned}\sum_{U\subseteq[t]\colon |U|=m}\|\mathbf{y}_U\|^2 &= \sum_{U\subseteq[t]\colon |U|=m}\left\|\sum_{i\in U}\mathbf{x}^{(i)}\right\|^2\\ &= \sum_{U\subseteq[t]\colon |U|=m}\left(\sum_{i\in U}\left\|\mathbf{x}^{(i)}\right\|^2 + \sum_{i,j\in U\colon i\neq j}\left\langle\mathbf{x}^{(i)},\mathbf{x}^{(j)}\right\rangle\right),\end{aligned}$$

and since $||\mathbf{x}^{(i)}|| \leq 1$,

$$\sum_{U\subseteq[t]\colon |U|=m}\|\mathbf{y}_U\|^2 \leq \sum_{U\subseteq[t]\colon |U|=m}\left(m + \sum_{i,j\in U\colon i\neq j}\left\langle\mathbf{x}^{(i)},\mathbf{x}^{(j)}\right\rangle\right).$$

From the fact that a pair of vectors is contained in exactly $\binom{t-2}{m-2}$ m-tuples, it follows that

$$\sum_{U\subseteq[t]\colon |U|=m}\|\mathbf{y}_U\|^2 = \binom{t}{m}m + \binom{t-2}{m-2}\sum_{i,j\in[t]\colon i\neq j}\left\langle\mathbf{x}^{(i)},\mathbf{x}^{(j)}\right\rangle.$$

By adding the positive term $\binom{t-2}{m-2}\sum_{i\in[t]}$, we get

$$\begin{aligned}&\sum_{U\subseteq[t]\colon |U|=m}\|\mathbf{y}_U\|^2\\ &\quad\leq \binom{t}{m}m + \binom{t-2}{m-2}\sum_{i,j\in[t]\colon i\neq j}\left\langle\mathbf{x}^{(i)},\mathbf{x}^{(j)}\right\rangle + \binom{t-2}{m-2}\sum_{i\in[t]}\left\|\mathbf{x}^{(i)}\right\|^2\\ &\quad= \binom{t}{m}m + \binom{t-2}{m-2}\left\|\sum_{i\in[t]}\mathbf{x}^{(i)}\right\|^2\\ &\quad= \binom{t}{m}m + \binom{t-2}{m-2}t^2\|\mathbf{c}\|^2\\ &\quad\leq \binom{t}{m}m + \binom{t}{m}m^2\|\mathbf{c}\|^2.\end{aligned}$$

And putting the three terms in (2) together we get

$$\sum_{U\subseteq[t]\colon |U|=m} \|\mathbf{y}_U - m\mathbf{c}\|^2 \le \binom{t}{m} m.$$

□

Now we are ready to prove the new upper bound on the rate of Euclidean superimposed codes.

Proof of Theorem 1. Take an arbitrary Euclidean superimposed code $\mathcal{C}$ for t total users out of which at most m are active. Let n denote the length of the code, and – similarly to the above lemma – let $\mathbf{c} = \frac{1}{t}\sum_{i\in[t]} \mathbf{x}^{(i)}$. Let U be a random variable with uniform distribution over the m sized subsets of $[t]$.

$$\mathbf{P}(U = V) = \frac{1}{\binom{t}{m}} \qquad \forall V \subseteq [t]\colon |V| = m.$$

By the definition of expected value,

$$\mathbf{E}||\mathbf{y}_U - m\mathbf{c}||^2 = \frac{1}{\binom{t}{m}} \sum_{V\subseteq[t]\colon |V|=m} \|\mathbf{y}_V - m\mathbf{c}\|^2,$$

and using Lemma 1:

$$\mathbf{E}||\mathbf{y}_U - m\mathbf{c}||^2 \le m.$$

Jensen's inequality [1966], for the random variable $||\mathbf{y}_U - m\mathbf{c}||$ says

$$\left(\mathbf{E}\left(\|\mathbf{y}_U - m\mathbf{c}\|\right)\right)^2 \le \mathbf{E}\left(\|\mathbf{y}_U - m\mathbf{c}\|^2\right),$$

so

$$\mathbf{E}\|\mathbf{y}_U - m\mathbf{c}\| \le \sqrt{m}.$$

Thus by Markov's inequality [1966],

$$\mathbf{P}\left(\|\mathbf{y}_U - m\mathbf{c}\| > 2\sqrt{m}\right) \le \frac{\mathbf{E}\left(\|\mathbf{y}_U - m\mathbf{c}\|\right)}{2\sqrt{m}} = \frac{1}{2}.$$

This means that at least half of the m active user's sum vectors lies within an n-dimensional sphere of radius $2\sqrt{m}$.

But $\mathcal{C}$ is a Euclidean code, which means that even those received vectors within the sphere of radius $2\sqrt{m}$ must have distance at least d from each other. Applying the sphere packing argument to these vectors we get that

$$\frac{1}{2}\binom{t}{m} \leq \left(\frac{2\sqrt{m}+\frac{d}{2}}{\frac{d}{2}}\right)^n,$$

thus

$$\frac{1}{2}\left(\frac{t}{m}\right)^m \leq \left(1+\frac{4\sqrt{m}}{d}\right)^n,$$

and by taking the logarithm,

$$n \geq \frac{\log\frac{1}{2}+m(\log t-\log m)}{\log\left(1+\frac{4\sqrt{m}}{d}\right)},$$

and this also holds for the shortest possible Euclidean code with given parameters:

$$N_E(t,m,d) \geq \frac{\log\frac{1}{2}+m(\log t-\log m)}{\log\left(1+\frac{4\sqrt{m}}{d}\right)},$$

thus

$$\liminf_{m\to\infty}\liminf_{t\to\infty}\frac{N_E(t,m,d)\log m}{m\log t} \geq 2.$$

□

Theorem 2. *(Ericson–Györfi, [1988])*

$$\limsup_{m\to\infty}\limsup_{t\to\infty}\frac{N_E(t,m,d)\log m}{m\log t} \leq 4,$$

i.e.,

$$N_E(t,m,d) \lesssim \frac{4m\log t}{\log m}.$$

Notice that there is still an exponential gap between the bounds given in Theorems 1 and 2 in terms of the maximum number of possible codewords. The lower bound gives only the square root of the upper bound.

Proof. The proof is based on random coding. Choose a random code for t total and m active users with length n with the following distribution:

$$\mathbf{P}\left(\left\{\mathbf{X}_j^{(i)}=\frac{1}{\sqrt{n}}\right\}\right)=\mathbf{P}\left(\left\{\mathbf{X}_j^{(i)}=-\frac{1}{\sqrt{n}}\right\}\right)=\frac{1}{2} \qquad \forall i\in[t]\ \forall j\in[n].$$

For the probability of that this code does not have minimal distance d, we have

$$\begin{aligned}\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) &= \mathbf{P}\left(d^2_{\min}(\mathcal{C}) < d^2\right)\\ &= \mathbf{P}\left(\min_{(U,V)\in A_{t,m}} \|\mathbf{y}_U - \mathbf{y}_V\|^2 < d^2\right),\end{aligned}$$

where

$$A_{t,m} = \big\{(U,V)\colon U \subseteq [t], V \subseteq [t], |U| \le m, |V| \le m, U \neq V\big\}.$$

Since for each pair (U,V) setting the minimum, the disjoint pair $(U \setminus U \cap V, V \setminus U \cap V)$ also sets the minimum, it is enough to take into account the disjoint sets only:

$$\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) = \mathbf{P}\left(\min_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset}} \|\mathbf{y}_U - \mathbf{y}_V\|^2 < d^2\right),$$

and applying the union bound, we get

$$\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) \le \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset}} \mathbf{P}\left(\|\mathbf{y}_U - \mathbf{y}_V\|^2 < d^2\right).$$

Since the codewords are composed of components $\pm\frac{1}{\sqrt{n}}$, if $|U| + |V|$ is odd, then

$$\big|[\mathbf{y}_U - \mathbf{y}_V]_j\big| \ge \frac{1}{\sqrt{n}} \qquad \forall j \in [n],$$

so $\|\mathbf{y}_U - \mathbf{y}_V\| \ge 1$. Thus for $|U| + |V|$ odd for $d \le 1$, the probability

$$\mathbf{P}\left(\|\mathbf{y}_U - \mathbf{y}_V\|^2 < d^2\right) = 0,$$

so we do not have to sum these cases. For $|U| + |V|$ even

$$\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) \le \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} \mathbf{P}\left(\|\mathbf{y}_U - \mathbf{y}_V\|^2 < d^2\right).$$

Moreover, for $U \cap V = \emptyset$ the distributions of $\mathbf{y}_U - \mathbf{y}_V$ and $\mathbf{y}_U + \mathbf{y}_V$ are the same, i.e.:

$$\begin{aligned}\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) &\le \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} \mathbf{P}\left(\|\mathbf{y}_U + \mathbf{y}_V\|^2 < d^2\right)\\ &= \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} \mathbf{P}\left(\left\|\sum_{i\in U\cup V}\mathbf{X}^{(i)}\right\|^2 < d^2\right)\\ &= \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} \mathbf{P}\left(n\sum_{j=1}^{n}\left(\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}\right)^2 < nd^2\right),\end{aligned}$$

and by the Chernoff bounding technique,

$$\begin{aligned}\mathbf{P}\big(d_{\min}(\mathcal{C}) < d\big) &= \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} \mathbf{P}\left(\exp\left(-\frac{n}{2}\sum_{j=1}^{n}\left(\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}\right)^2\right) > e^{-\frac{nd^2}{2}}\right)\\ &\le \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} e^{\frac{nd^2}{2}}\mathbf{E}\left(\exp\left(-\frac{n}{2}\sum_{j=1}^{n}\left(\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}\right)^2\right)\right)\\ &= \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} e^{\frac{nd^2}{2}}\prod_{j=1}^{n}\mathbf{E}\left(\exp\left(-\frac{1}{2}\left(\sqrt{n}\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}\right)^2\right)\right)\\ &= \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V| \text{ is even}}} e^{\frac{nd^2}{2}}\left(\mathbf{E}\left(\exp\left(-\frac{1}{2}\left(\sqrt{n}\sum_{i\in U\cup V}\mathbf{X}_1^{(i)}\right)^2\right)\right)\right)^n.\end{aligned}$$

If $|U|+|V|$ is even, then $\sqrt{n}\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}$ is also even, with distribution

$$\mathbf{P}\left(\sqrt{n}\sum_{i\in U\cup V}\mathbf{X}_j^{(i)} = 2z\right) = \binom{2k}{k+z}\frac{1}{2^{2k}}$$

over $z\in\{-k,\dots,k\}$, where $2k = |U|+|V|$. Thus

$$\mathbf{E}\left(\exp\left(-\frac{1}{2}\left(\sqrt{n}\sum_{i\in U\cup V}\mathbf{X}_j^{(i)}\right)^2\right)\right) = \sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}\frac{1}{2^{2k}}.$$

So the Chernoff-bound is

$$\mathbf{P}(d_{\min}(\mathcal{C}) < d) \leq \sum_{\substack{(U,V)\in A_{t,m}\\ U\cap V=\emptyset\\ |U|+|V|=2k}} e^{\frac{nd^2}{2}} \left(\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}\frac{1}{2^{2k}}\right)^n,$$

where we enumerate the appropriate pairs (U,V) with respect to $2k = |U| + |V|$:

$$\mathbf{P}(d_{\min}(\mathcal{C}) < d) \leq \sum_{k=1}^{m}\binom{t}{2k}2^{2k}e^{\frac{nd^2}{2}} \left(\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}2^{-2k}\right)^n,$$

and since $\binom{t}{2k}2^{2k} \leq 2t^{2k}$ and $d \leq 1$,

$$\mathbf{P}(d_{\min}(\mathcal{C}) < d) \leq 2\sum_{k=1}^{m} t^{2k}e^{\frac{n}{2}} \left(\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}2^{-2k}\right)^n = 2(A+B),$$

where

$$A = t^2 e^{\frac{n}{2}} \left(\sum_{z=-1}^{1} e^{-2z^2}\binom{2}{1+z}2^{-2}\right)^n,$$

and

$$B = \sum_{k=2}^{m} t^{2k}e^{\frac{n}{2}} \left(\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}2^{-2k}\right)^n.$$

We will derive upper bounds on A and B:

$$\begin{aligned} A &= \exp\left(2\log t + n\left(\frac{1}{2} + \log(1+e^{-2}) - \log 2\right)\right) \\ &\leq \exp\left(2\log t - 0.066n\right). \end{aligned}$$

For B, we will use $\binom{2k}{k+z} \leq \binom{2k}{k}$ and $\binom{2k}{k}2^{-2k} \leq \frac{1}{\sqrt{\pi k}}$ (e.g. [1968]):

$$\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}2^{-2k} \leq \frac{1}{\sqrt{\pi k}}\sum_{z=-k}^{k} e^{-2z^2},$$

and using $\exp(-2z^2) \leq \exp(-2|z|)$, we get

$$\begin{aligned}\sum_{z=-k}^{k} e^{-2z^2}\binom{2k}{k+z}2^{-2k} &\le \frac{1}{\sqrt{\pi k}}\sum_{z=-k}^{k} e^{-2|z|}\\ &= \frac{1}{\sqrt{\pi k}}\left(1+2\sum_{z=1}^{k} e^{-2z}\right)\\ &\le \frac{1}{\sqrt{\pi k}}\left(1+2\frac{e^{-2}}{1-e^{-2}}\right)\\ &\le \frac{0.741}{\sqrt{k}}.\end{aligned}$$

So for B, we have

$$\begin{aligned}B &\le \sum_{k=2}^{m} t^{2k} e^{\frac{n}{2}}\left(\frac{0.741}{\sqrt{k}}\right)^n\\ &\le m \max_{k=2\ldots m} \exp\left(2k\log t + n\left(0.201-\frac{\log k}{2}\right)\right).\end{aligned}$$

It can be easily seen, that the exponent is convex in k. So the maximum is either at $k=2$ or at $k=m$:

$$B \le m\max\{C,D\},$$

where

$$\begin{aligned}C &= \exp\left(4\log t + n\left(0.201-\frac{\log 2}{2}\right)\right)\\ &\le \exp\left(4\log t - 0.145n\right),\end{aligned}$$

and

$$D = \exp\left(2m\log t + n\left(0.201-\frac{\log m}{2}\right)\right).$$

We want to show that for large values of t, the probability of that this random code does not have a certain minimal distance is less than one. We have $\mathbf{P}\left(d_{\min}(\mathcal{C}) < d\right) \le 2(A + m\min\{B,C\})$, so it is enough to show that

$$\lim_{t\to\infty} A = 0, \lim_{t\to\infty} C = 0 \text{ and } \lim_{t\to\infty} D = 0.$$

Set $n = \lceil c(m)\log t\rceil$, then

$$\begin{aligned}A &\le \exp\left(\left(2-0.066c(m)\right)\log t\right),\\ C &\le \exp\left(\left(4-0.145c(m)\right)\log t\right),\end{aligned}$$

and

$$D \le \exp\left(\left(2m - \left(\frac{\log m}{2} - 0.201\right) c(m)\right) \log t\right).$$

All these quantities A, B and C tend to 0 as $t \to \infty$ if in the exponents $\log t$ has a negative factor. We have this for A if $c(m) > 30.304$, for C if $c(m) > 27.587$, and for D if

$$2m - \left(\frac{\log m}{2} - 0.201\right) c(m) < 0.$$

All of these conditions are satisfied by

$$c(m) = \frac{4(1+\varepsilon)m}{\log m}$$

for $m \ge 25$ and $m \ge \exp\left(\frac{0.402(1+\varepsilon)}{\varepsilon}\right)$, where $\varepsilon > 0$ arbitrary.

Summarizing, we have shown that for any $\varepsilon > 0$, if

$$m > \max\left\{25, \exp\left(\frac{0.4005(1+\varepsilon)}{\varepsilon}\right)\right\},$$

the probability of a randomly selected code with length

$$n = \left\lceil \frac{4(1+\varepsilon)m}{\log m} \log t \right\rceil$$

not having minimal distance d tends to 0:

$$\lim_{t\to\infty} \mathbf{P}(d_{\min}(\mathcal{C}) < d) = 0.$$

This means that for t large enough, a good code with certain parameters exists, so for any $\varepsilon > 0$, m large enough and t large enough

$$N_E(t, m, d) < \frac{4(1+\varepsilon)m}{\log m} \log t + 1,$$

which implies that

$$\limsup_{m\to\infty} \limsup_{t\to\infty} \frac{N_E(t, m, d) \log m}{m \log t} \le 4.$$

□

3. Signature Coding and Information Transfer for the Euclidean Channel

There are t users of the channel: $\mathcal{U} = \{1, 2, \ldots, t\}$. Each user u has a component code, which is formed by s real valued codewords of length n:

$$C_u = \{\mathbf{x}^{(u,1)}, \mathbf{x}^{(u,2)}, \ldots, \mathbf{x}^{(u,s)}\},$$

each codeword is associated with a specific message of the user. We have an energy constraint: $\left\|\mathbf{x}^{(u,j)}\right\| \leq 1$, where $\|.\|$ denotes the Euclidean norm. At a given instant, there are some (say r) active users. They are denoted by the set U. Enumerate them as $U = \{u_1, u_2, \ldots, u_r\}$, where $u_1 < u_2 < \ldots < u_r$. We consider, that at any time at most m users are active, so $r \leq m$. For each active user $u_i \in U$, let $m_i \in \{1, 2, \ldots, s\}$ denote the message this user wants to send. Form a vector of length r from the messages as $\mathbf{m} = \big(m_1, m_2, \ldots, m_r\big)$. The pair $(U, \mathbf{m})$, which is the set of active users and the vector of their messages together, is called a message constellation.

The active users send their corresponding codewords to the channel: user u_i with message m_i sends $\mathbf{x}^{(u_i,m_i)}$. The receiver gets the sum of the codewords sent, which is denoted by $\mathbf{S}(U, \mathbf{m})$:

$$\mathbf{S}(U, \mathbf{m}) = \sum_{i=1}^{r} \mathbf{x}^{(u_i,m_i)}.$$

If the code $\mathcal{C}$ is such that for each different pair $(U, \mathbf{m})$, the channel output is different at least by d in Euclidean norm, then this code has distance d. Formally,

$$\|\mathbf{S}(U, \mathbf{m}) - \mathbf{S}(V, \mathbf{n})\| < d \iff (U = V \text{ and } \mathbf{m} = \mathbf{n})$$
$$\forall U, V, \mathbf{m}, \mathbf{n} \colon |U| \leq m, |V| \leq m.$$

Given t, m, s and d, the smallest codeword length for which a d-distance s-message Euclidean code $\mathcal{C}$ for t total users out of which at most m are active exists is noted by $N(t, m, s, d)$.

An analogue of Theorem 1 of Füredi and Ruszinkó for this case can be stated as follows

Theorem 3. *(Laczay, [2005])*

$$\liminf_{m\to\infty} \liminf_{ts\to\infty} \frac{N(t, m, s, d) \log m}{m \log ts} \geq 2,$$

i.e.,

$$N(t, m, s, d) \gtrsim \frac{2m \log ts}{\log m}.$$

To prove this theorem, we taylor Lemma 1 to our needs:

Lemma 2. *(Laczay, [2005]) For arbitrary code $\mathcal{C}$ defined above, the inequality*

$$\sum_{\substack{U\subseteq[t]:\,|U|=m\\ \mathbf{m}\in\{1,2,\dots,s\}^m}} \|\mathbf{S}(U,\mathbf{m})-m\mathbf{c}\|^2 \le \binom{t}{m}s^m m$$

holds, where

$$\mathbf{c}=\frac{1}{ts}\sum_{\substack{i\in\{1,2,\dots,t\}\\ k\in\{1,2,\dots,s\}}}\mathbf{x}^{(i,k)}$$

is the average vector.

Proof. The proof is similar to the proof of Lemma 1. □

Proof of Theorem 3. Similarly to the proof of Theorem 1, combine Lemma 2 with the sphere packing argument by using Markov's and Jensen's inequalities. □

For the upper bound, consider that an Euclidean signature code with $t'=ts$ users (and so with $t'=ts$ codewords) is also an s-message Euclidean code for t users. This is because for a signature code with $t'=ts$ users we required that all sum of at most m codewords should be distinct by distance d. For an s message code for t users we require that only those at most m sums must be distinct, which has at most one codeword from all component code. Thus Theorem 2 of Ericson and Györfi provides an upper bound also for the minimal codeword length of s-message Euclidean codes, that is

Corollary 1. *(Laczay, [2005])*

$$2\le\limsup_{m\to\infty}\limsup_{ts\to\infty}\frac{N(t,m,s,d)\log m}{m\log ts}\le 4.$$

i.e.,

$$\frac{2m\log ts}{\log m}\lesssim N(t,m,s,d)\lesssim\frac{4m\log ts}{\log m}.$$

4. Constructions of superimposed codes for the Euclidean channel

Until now we considered only the asymptotic behavior of the function $N_E(t,m,d)$ for large t and m. In this section we present several constructions of Euclidean signature codes. These are exclusively representing sets of points on the unit sphere Ω_n formally defined as

$$\Omega_n\stackrel{\text{def}}{=}\{\mathbf{x}\in\mathbb{R}^n\mid||\mathbf{x}||=1\}.$$

In other words we limit ourselves to considering signature codewords of unit energy. Such constellations are known as *spherical codes* and have been extensively studied in the literature. (See, e.g., the excellent book of Ericson and Zinoviev [2001] on this

subject.) Recall that three most important parameters of a spherical codes are dimension, cardinality and minimum distance. Spherical code C which satisfies the conditions of Definition 1 will be refered to as *spherical superimposed code* and will be denoted as (n, d, m, t)-SSC.

It is clear from the definitions that an (n, d, m, t)-SSC is also an (n, d', m, t)-SSC for every $d' < d$. In most of the constructions of SSCs presented here the exact determination of the minimum distance is impossible. A lower bound on d is computed instead.

We start with some basic constructions.

Construction 1. *An orthonormal basis of $\mathbb{R}^n$ forms a $(n, 1, n, n)$-SSC.*

We can actually accommodate one more user while keeping the same dimension, minimum distance and number of active users. This can be done in the following manner. The points that form an orthonormal basis of $\mathbb{R}^{n+1}$ lie on a hyperplane of dimension n. By projecting them onto $\mathbb{R}^n$ and some re-scaling we obtain the so-called simplex code on Ω_n. It can be easily checked that the following is true.

Construction 2. *A simplex code on Ω_n forms a $(n, 1, n, n+1)$-SSC.*

Before proceeding with more advanced constructions we give one way to obtain SSCs in two dimensions.

Construction 3. *A regular n-gon on Ω_2 forms a $(2, d, k-1, n)$-SSC, where $d > 0$ and k is the least non-unit divisor of n.*

The drawback of Construction 3 is that the actual minimum distance is difficult to compute.

A powerful method for deriving SSCs is to use certain mappings from the set $\{0, 1, \ldots, p-1\}$ into $\mathbb{R}$ or $\mathbb{R}^2$. Examples of such mappings are the following.

$$\begin{aligned}
\mathbf{AM1} &: f_1^{(n)}(x) = \frac{x}{\sqrt{n}(p-1)}, \\
\mathbf{AM2} &: f_2^{(n)}(x) = \frac{1}{\sqrt{n}}\left(1 - \frac{2x}{p-1}\right), \\
\mathbf{PhM} &: f_3^{(n)}(x) = \frac{1}{\sqrt{n}}\left(\cos\frac{2\pi x}{p}, \sin\frac{2\pi x}{p}\right).
\end{aligned}$$

The first more advanced construction of SSCs is described in [1988].

Construction 4. (The EG construction) *Let C_b be a binary linear $[N, K, D]$-code which contains the all-one word. Let $\overline{C_b}$ be the set that is obtained from C_b by deleting all words starting with 1 and deleting the first coordinate from the rest. Suppose that*

$$D \geq d_0 \stackrel{\text{def}}{=} \frac{a^2(n+2) - 2a(n+1) + d^2 n}{2a(a-1)} \tag{3}$$

for some d, $0 < d \leq 1$, where $a \stackrel{\text{def}}{=} \min\{t, 2m\}$ and $n = N - 1$. Applying the mapping **AM2** *to $\overline{C_b}$, we obtain (n, d, m, t)-SSC.*

This construction can be generalized. The main idea is to find some necessary conditions for a spherical code to posses certain superimposed properties. We define a non-negative valued function $g(m,t,s_1,s_2)$ in the following manner. Let $g(m,t,s_1,s_2) = g_i(m,t,s_1,s_2)$ whenever $(m,t,s_1,s_2) \in M_i \subset \mathbb{Z}_+^2 \otimes \mathbb{R}^2,\ i = 1,2,3,4,5,6$. The functions $g_i(m,t,s_1,s_2)$ are defined as

$$g_i^2(m,t,s_1,s_2) = \begin{cases} (2m^2+t^2-2mt-t)s_1 + 2m(m-t)s_2 + t, & \text{if } i=1, \\ (t(t-2)s_1 - t^2 s_2 + 2t)/2, & \text{if } i=2, \\ 2m((m-1)s_1 - ms_2 + 1), & \text{if } i=3, \\ m((m-1)s_1+1), & \text{if } i=4, \\ 1, & \text{if } i=5, \\ 0, & \text{if } i=6. \end{cases}$$

The regions M_i, $i = 1,\dots,6$ depend on the choice of parameters m, t, s_1 and s_2. Their description is given below.

$$M_1 = \{(m,t,s_1,s_2) \mid -\frac{1}{m-1} \le s_1 \le -\frac{1}{t},\ \frac{(t-m-1)s_1+1}{2m} \le s_2 \le -s_1,$$
$$\frac{(t-1)(ts_1+1)}{2m(t-m)} - s_1 \le s_2 \le \frac{t((t-1)s_1+1)}{2m(t-m)} - s_1,\ m < t < 2m\},$$

$$M_2 = \{(m,t,s_1,s_2) \mid m \le t < 2m,\ -\frac{1}{t-1} \le s_1 \le 0,\ s_2 \ge -s_1,$$
$$\frac{t(t-2)s_1 + 2(t-1)}{t^2} \le s_2 \le \frac{(t-2)s_1+2}{t}\},$$

$$M_3 = \{(m,t,s_1,s_2) \mid 4 \le 2m \le t, -\frac{1}{m-1} \le s_1 \le 0, s_2 \ge \frac{(m-1)s_1+1}{2m},$$
$$\frac{(m-1)s_1+1}{m} - \frac{1}{2m^2} \le s_2 \le \frac{(m-1)s_1+1}{m}\},$$

$$M_4 = \{(m,t,s_1,s_2) \mid 2 \le m \le t,\ -\frac{1}{m-1} \le s_1 \le -\frac{1}{m},\ s_2 = s_1 \text{ if } t = m,$$
$$s_2 \le \frac{(a-m-1)s_1+1}{2m} \text{ if } m \ne t \text{ and } a = \min\{t, 2m\},\ s_2 \ge s_1\},$$

$$M_5 = \{(m,t,s_1,s_2) \mid 2 \le m \le t, s_2 \le (1-\frac{2}{t})s_1 + 2\frac{(t-1)}{t^2} \text{ if } m \le t < 2m,$$
$$s_2 \le \frac{(a-1)(as_1+1)}{2m(a-m)} - s_1 \text{ if } m \ne t \text{ and } a = \min\{t,2m\},\ s_2 \ge s_1,\ -\frac{1}{m} \le s_1 \le 0\},$$

$$M_6 = \mathbb{Z}_+^2 \otimes \mathbb{R}^2 \setminus \cup_{i=1}^5 M_i$$

The function $g(m,t,s_1,s_2)$ gives actually a lower bound on the minimum distance of a certain spherical code considered as a SSC. The result is given in the next statement.

Theorem 4. *Let $m \ge 2$ be an integer and C be a (n,t,d_0)-spherical code such that $\langle \mathbf{x},\mathbf{y}\rangle \in [s_1,s_2]$ for every $\mathbf{x} \ne \mathbf{y}$ in C. Then C is a $(n, d = g(m,t,s_1,s_2), m, t)$-SSC.*

n	d	m	t	n	d	m	t	n	$d \geq$	m	t	n	$d \geq$	m	t
6	1	2	8	11	1	3	14	6	0.453	2	12	12	0.930	3	17
7	1	2	10	12	1	3	16	7	0.819	2	14	12	0.342	3	20
8	1	2	13	13	1	3	19	9	0.442	2	30	13	0.831	3	20
9	1	2	18	14	1	3	20	10	0.554	2	40	14	0.993	3	21
10	1	2	20	15	1	3	23	11	0.289	2	54	14	0.808	3	23
11	1	2	26	16	1	3	26	11	0.161	2	60	15	0.985	3	24
12	1	2	39	12	1	4	14	12	0.826	2	48	15	0.227	3	30
13	1	2	52	13	1	4	15	13	0.808	2	54	16	0.600	3	31
14	1	2	54	14	1	4	16	14	0.999	2	55	11	0.663	4	13
15	1	2	50	15	1	4	18	8	0.719	3	10	13	0.663	4	16
16	1	2	50	16	1	4	20	9	0.719	3	12	14	0.947	4	17
9	1	3	11	15	1	5	17	10	0.530	3	14	15	0.776	4	19
10	1	3	12	16	1	5	18	11	0.483	3	17	14	0.648	5	16

Table 1. Spherical superimposed codes derived from the best codes in $\mathbf{G}(n,1)$ known.

The proof of Theorem 4 is more or less straightforward. Two particular cases of special interest need to be stated here. The first is when the interval $[s_1, s_2]$ is symmetric around the zero.

Corollary 2. *Let C be a (n,t,d_0)-spherical code with inner products within the interval $[s,-s]$, where $-1 \leq s \leq 0$. Let m be a positive integer and define $a = \min\{2m,t\}$. Then C is an $(n,1,m,t)$-SSC if $s \in [-1/a, 0]$ and $(n, \sqrt{a(1+(a-1)s)}, m, t)$-SSC if $s \in [-1/(a-1), -1/a]$.*

This corollary is especially applicable for spherical codes obtained from codes in the Grassmannian space $\mathbf{G}(n,1)$ consisting of all lines in $\mathbb{R}^n$ passing trough the origin. Constructions of codes in $\mathbf{G}(n,1)$ can be found in [1996]. Table 1 gives the parameters of some spherical superimposed codes obtained from these codes with help of the construction given above. The lower bound on the minimum distance is computed with help of Corollary 2.

The next interesting case is when we obtain superimposed codes with $d = 1$ and many points.

Corollary 3. *Let C be a (n,t,d_0)-spherical code with inner products in the interval $[s_1, s_2]$ and let $m \leq t/2$ be an integer number. If $s_1 \in \left[-\frac{1}{m}, 0\right]$ and $s_2 \in \left[s_1, \frac{((m-1)s_1+1)}{m} - \frac{1}{2m^2}\right]$ then C is a $(n,1,m,t)$-SSC.*

Based on this corollary we can assure the existence of $(q(q^2-q+1), 1, q-1, (q+1)(q^3+1))$-SSC for any prime power $q \geq 3$ due to the existence of a class of optimal spherical codes described of Levenshtein [1987]. It is also worth mentioning the existence of spherical superimposed codes with parameters $(21,1,2,162)$, $(22,1,2,100)$ and $(22,1,2,275)$, respectively.

We turn back to the mapping method and use p-ary representations of so-called A_s- and B_s-sets which give the following result.

Construction 5. (The A construction) *Given a primitive polynomial of degree $m+1$ over $GF(q)$, we can obtain (n,d,m,t)-SSC with $t=q+1$ and the following parameters, for any integer $r \geq 2$ and for $v=(q^{m+1}-1)/(q-1)$*

$$\begin{aligned}
&\mathbf{AM1}: n=\lfloor \log_r v \rfloor + 1,\ d=\frac{1}{\sqrt{n}(r-1)},\\
&\mathbf{AM2}: n=\lfloor \log_r v \rfloor + 2,\ d=\frac{2}{\sqrt{n}(r-1)},\\
&\mathbf{PhM}: n=2\lfloor \log_3 v \rfloor + 3,\ d=\sqrt{\frac{6}{n+1}}, r=3.
\end{aligned}$$

It is always interesting to show that some constructions are optimal in a certain sense. For example for given dimension n, cardinality t and maximal number of active users m we want to find the maximal minimum distance $d(n,m,t)$ that can be achieved, i.e. there exists an $(n,d(n,m,t),m,t)$-SSC and there is no (n,d,m,t)-SSC with $d>d(n,m,t)$. This is a rather difficult task in higher dimensions but we can actually state some such results for dimension 2.

In order to simplify the descriptions we introduce some notations. First we identify $\mathbb{R}^2$ with the set of complex numbers $\mathbb{C}$. Every point $(a,b)\in\mathbb{R}^2$ is associated with the number $a+ib=\rho e^{i\varphi}$, where $i^2=-1$. Every set on the unit circle can be represented by a set of angles $\varphi\in[0,2\pi)$ corresponding to its points. For example the set $\mathcal{C}_k \stackrel{\text{def}}{=} \{\varphi_j = 2j\pi/k,\ j=0,1,\ldots,k-1\}$ represents a regular k-gon which has vertex $(1,0)$.

A natural way of obtaining codes with even cardinalities is to take away one point from the regular polygon with one more vertex. However the following construction give better minimum distances.

Construction 6. *Let t be an even number which is not a power of 2. Let p be the smallest odd prime divisor of t. Choose the set $\mathcal{B}_p^t$ to be the subset of $\mathcal{C}_{2t}$ consisting of the angles*

$$\varphi_k^i=\left(\frac{2k}{p}+\frac{i}{t}\right)\pi,\ k=0,1,\ldots,p-1,\ i=0,1,\ldots,t/p-1.$$

The exact determination of the minimum distance of the codes $\mathcal{B}_p^t$ in the general case is still an open problem. The results for the case $p=3$ are described below.

Theorem 5. *Let t be a positive integer number divisible by 6. Then the codes $\mathcal{B}_3^t$ given in Construction 6 have parameters*
$(n,d,m,t)=(2,4\sin\frac{\pi}{t}\sin\frac{\pi}{2t},2,t)$.

Proof. Let B be the set all sums of up to two different vectors in $\mathcal{B}_3^t$ including the all-zero vector. We observe that the set B is preserved by the rotations through angle $2\pi/3$ and center in the origin. It is also kept by the reflections in the lines along the vectors corresponding to the angles $\dfrac{(2i+1)t-3}{6t}\pi$, $i=0,1,2$. Thus we can consider the non-zero points of B which correspond to angles in the interval $[0,2\pi/3]$. These points can be divided in three sets defined as $B_1=\{\varphi_0^i \mid i=0,1,\ldots,t/3-1\}$, $B_2=\{\varphi_0^i+$

$\varphi_0^j \mid i,j = 0,1,\ldots,t/3-1,\ i \neq j\}$ and $B_3 = \{\varphi_0^i + \varphi_1^j \mid i,j = 0,1,\ldots,t/3-1\}$. It is easy to see that the distance between two points from different sets as well as the distance of every point to the origin is at least $2\sin\frac{\pi}{2t}$, which is the side-length of the regular $2t$-gon. Further the points of B_3 can be divided in "levels" by their Euclidean norm. The minimum distance between the different levels is $2\sin\frac{\pi}{2t}$ and between the points on the level of radius r is $2r\sin\frac{\pi}{2t}$. The innermost level with at least 2 points has $r = 2\sin\frac{\pi}{t}$ and thus $d_{\min}(B_3) = 4\sin\frac{\pi}{t}\sin\frac{\pi}{2t}$. By similar arguments we can deduce $d_{\min}(B_2) = 4\sin\frac{\pi}{t}\sin\frac{\pi}{2t}$. Clearly $d_{\min}(B_1) = 2\sin\frac{\pi}{2t}$ which concludes the proof. □

For the case $p > 3$ we claim that the minimum distance of the constructed codes is non-zero. Before proceeding with the proof of this fact we need the following lemma.

Lemma 3. *Let t be an even positive number that is not a power of 2 and p be its least odd prime divisor. Then there are no opposite vectors in $\mathcal{B}_p^t$, i.e. vectors with zero sum. Moreover all regular p-gons with vertices in $\mathcal{C}_{2t}$ are either completely included or does not have points in $\mathcal{B}_p^t$.*

Proof. Suppose first that there are opposite points in $\mathcal{B}_p^t$. Then

$$\pi = |\varphi_k^i - \varphi_l^j| = \left|\frac{2(k-l)}{p} - \frac{i-j}{t}\right|\pi,$$

for some integers i,j,k,l such that $i,j \in [0,t/p-1]$ and $k,l \in [0,p-1]$. This is impossible since p is an odd number and $|i-j|/t < 1/p$. The second part follows directly from the easy observation that all regular p-gons, which are subsets of $\mathcal{C}_{2t}$ are $\{\varphi_k^i\}_{k=0}^{p-1}$ for $i = 0,1,\ldots,2t/p-1$. □

Now we can state the main result concerning Construction 6.

Theorem 6. *The codes $\mathcal{B}_p^t$ described in Construction 6 are $(2,d,p-1,t)$-SSCs where $d > 0$.*

Proof. Suppose that $d = 0$, which means that we have two different sets M and N of up to $p-1$ points in $\mathcal{B}_p^t$ which have the same sum. We can assume that $M \cap N = \emptyset$. Let us denote by $\overline{N}$ the set of opposite vectors to those in N. Then the sum of the vectors in $M \cup \overline{N}$ is the zero-vector. Since $M \cup \overline{N} \subseteq \mathcal{C}_{2t}$ this can happen only if the points in $M \cup \overline{N}$ are all the vertices of a regular l-gon, where $l|t$ and $l \geq 2$. We have $1 \leq |M \cup \overline{N}| \leq 2(p-1)$ and from the definition of t and p we get two possible cases, namely $|M \cup \overline{N}|$ even or $|M \cup \overline{N}| = p$. Both cases are excluded by Lemma 3. □

Since the angle between any two lines trough the origin and the points of a $(2,d,m,t)$-SSC with $m \geq 2$ must be at least $2\arcsin(d/2)$ we obtain the following upper bound on the minimum distance of such a code.

Proposition 1. *If there exists a $(2,d,m,t)$-SSC with $m \geq 2$ and $t \geq 3$, then $d \leq 2\sin(\pi/(2t))$.*

Proof. The only thing we must see is the obvious fact that the minimum angle between t lines trough the origin in $\mathbb{R}^2$ is at most π/t. □

$\mathbf{t}$	$\mathbf{d_3}$	$\mathbf{d_6}$	$\mathbf{d_{ub}}$
6	0.24697960	0.51763809	0.51763809
10	0.16037889	0.17557050	0.31286893
12	0.11538526	0.13513066	0.26105238
14	0.08693075	0.09965775	0.22392895
18	0.05436845	0.06053774	0.17431149
20	0.04455177	0.04909482	0.15691819
22	0.03716936	0.04061049	0.14267837
24	0.03147895	0.03414728	0.13080626
26	0.02700081	0.02911129	0.12075699
28	0.02341378	0.02511159	0.11214089

Table 2. Comparison of Construction 3 and Construction 6 for codes of dimension $n = 2$ and order $m = 2$.

$\mathbf{n}$	$\mathbf{m}$	$\mathbf{T}$	$\mathbf{d(n, m, T)}$
2	2	4	$2\sin(\pi/10) \approx 0.61802399$
2	2	5	$2\sin(\pi/12) \approx 0.51763809$
2	2	6	$2\sin(\pi/12) \approx 0.51763809$

Table 3. Known d-optimal spherical superimposed codes with $d < 1$.

For the special case of $m = 2$ the bound from Proposition 1 is asymptotically better then the sphere packing bound, discussed in the second section, as $t \to \infty$. It is not surprising that for larger m we have the opposite situation. A natural explanation is that the limitation on the angles of the lines is quite weak in those cases.

Table 2 shows the advantages of Construction 6 to Construction 3. The notation d_i refers to the minimum distance of the codes obtained from the corresponding construction. The codes from Construction 3 are obtained by removing one point from the vertices of a regular $(t + 1)$-gon. We list also the corresponding upper bound obtained by Proposition 1 in the last column of the table.

Other possibilities for choosing some points of $\mathcal{C}_k$ to obtain $(2, d, m, t)$-SSCs can be investigated. This idea is promising as we can see from the following example.

Example 1. *The code* $\mathcal{C}_{10}^{0,1,4,7}$ *consisting of vectors corresponding to the angles* $0, \pi/5, 4\pi/5$ *and* $7\pi/5$*, which is a subset of* $\mathcal{C}_{10}$ *is a* $(2, 2\sin(\pi/10), 2, 4)$*-SSC.*

It is possible to show that the code in Example 1 satisfies $d(2, 2, 4) = 2\sin(\pi/10)$. With the aid of the bound from Proposition 1 we are able to determine two more values of the function $d(n, m, T)$, namely $d(2, 2, 3) = 1$ and $d(2, 2, 6) = 2\sin(\pi/12)$. The codes achieving these values are $\mathcal{C}_3$ and $\mathcal{B}_3^6$, respectively. Observe that $\mathcal{C}_3$ is d_2-optimal, but clearly not d_3-optimal. Further geometrical reasons reveal that $d(2, 2, 5) = d(2, 2, 6) = 2\sin(\pi/12)$. The known cases of d_m-optimal codes with $d < 1$ are summarized in Table 3.

5. Signature codes in other normed spaces

So far in this chapter we presented results for Euclidean codes. We will shortly outline here that these results can be extended to arbitrary normed spaces.

Let $\mathcal{N} = (X, ||\cdot||)$ be a finite-dimensional (n-dimensional) normed vector space, and let $B(\mathbf{c}, r)$ denote the closed ball with center $\mathbf{c}$ and radius $r > 0$. We also use B for the unit-ball $B(\mathbf{0}, 1)$ of $\mathcal{N}$. In general, this B may also be considered as an arbitrary n-dimensional symmetric convex body in $\mathbb{R}^n$, the symmetry being with respect to the origin. One might also be interested in the growth rate of normed signature codes in the more general normed vector space $\mathcal{N}$, where the norm is defined by an arbitrary n-dimensional central symmetric convex body. Similarly to the Euclidean norm case, this means the following.

Let $\mathcal{C}$ be a finite set of (at most) unit norm vectors in $\mathcal{N}$, it is called a normed signature code in $\mathcal{N}$ with parameters (n, m, t, d) if $|\mathcal{C}| = t$ and for two arbitrary distinct subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{C}$ with $0 \le |\mathcal{A}|, |\mathcal{B}| \le m$ the $\mathcal{N}$-distance of the vectors $f(\mathcal{A})$ and $f(\mathcal{B})$ is at least d. (Here $f(\mathcal{A})$ and $f(\mathcal{B})$ is the sum of vectors in $\mathcal{A}$ and $\mathcal{B}$, respectively.) That is

$$d_{\mathcal{N}}(\mathcal{C}^m) := \min_{\substack{\mathcal{A}\neq\mathcal{B} \\ 0\le|\mathcal{A}|,|\mathcal{B}|\le m \\ \mathcal{A},\mathcal{B}\subseteq\mathcal{C}}} ||f(\mathcal{A}) - f(\mathcal{B})||_{\mathcal{N}} \ge d.$$

As before, for given t, m and d, let $n_{\mathcal{N}}(t, m, d)$ denote the minimum length of such a code.

We are able to extend the bounds of Theorems 1 and 2 for all finite-dimensional normed spaces, $\mathcal{N}$, in a somewhat weaker form.

Theorem 7. *(Füredi–Ruszinkó, [1999])*

$$\frac{n_{\mathcal{N}}(t, m, d)}{\log t} = \Theta\left(\frac{m}{\log m}\right). \tag{4}$$

Here Θ is used in the conventional sense, i.e., for sequences $f(m)$ and $g(m)$, $f(m) = \Theta(g(m))$ if $f(m) \le c_1 g(m)$ and $f(m) \ge c_2 g(m)$ hold with appropriate positive constants $c_1,\ c_2$ and every m.

Proof. (Sketch) To prove the upper bound (4) use the following theorem of Milman [1985]. For every $\varepsilon > 0$ there exists a positive constant $\psi(\varepsilon) > 0$, such that one can find a projection of a section of B (say, $\Pi_{F_2}(F_1 \cap B)$ with $F_2 \subset F_1 \subset \mathbf{R}^n$) which is $(1+\varepsilon)$-equivalent to an ellipsoid and has dimension at least $\psi(\varepsilon)n$. Here the ψ is independent from the convex body B, but, of course, the choice of the subspaces, F_1 and F_2, varies with B. (For more background on this topic and proofs see the excellent book of Pisier [1989]). An ellipsoid is affine invariant to the Euclidean ball, so taking a Euclidean signature code $\mathcal{C}$, of maximum size in the subspace F_2 – by the affine invariant transformation mapping the unit ball to the ellipsoid – we will get a signature code with the same parameters with respect to the distance defined by the ellipsoid. Project $\mathcal{C}$ back to $F_1 \cap B$, and – by Milman's theorem – obtain a signature code in $\mathcal{N}$ with parameters $(n, m, |\mathcal{C}|, d/(1+\varepsilon))$.

The upper bound in (4) easily follows from the volume bound of Ericson and Györfi [1988],

$$\binom{T}{m} \leq \left(\frac{m+d/2}{d/2}\right)^n,$$

which is true for every space $\mathcal{N}$ and every t, n, m and d. □

References

[1996] J. H. Conway, R. H. Hardin, and N. J. A. Sloane. Packing Lines, Planes, etc., Packings in Grassmannian Spaces. *Experimental Mathematics*, 5:139–159, 1996.

[1988] Ericson, T. and Györfi, L. (1988). Superimposed codes in R^n. *IEEE Transactions on Information Theory*, IT-34(4):877–880.

[2001] Ericson, T and Zinoviev, V. *Codes on Euclidean Spheres.* Elsevier, North-Holland Mathematical Library, 2001

[1966] Feller, W. (1966) *An Introduction to Probability Theory and Its Applications.* 2nd ed. New York: John Wiley & Sons, 1966.

[1999] Füredi, Z. and Ruszinkó, M. (1999). An improved upper bound of the rate of euclidean superimposed codes. *IEEE Transactions on Information Theory*, IT-45(2):799–802.

[1968] Gallager, R. G. (1968). *Information Theory and Reliable Communication*. John Wiley & Sons.

[2005] Laczay, B. (2005) Private communication

[1987] Levenshtein, V. I. Packing of Polynomial Metric Spaces. In *Proceedings of the Third International Workshop on Information Theory*, pages 271–274, Sochi, 1987.

[1985] Milman, V. D. Almost Euclidean quotient spaces of subspaces of finite dimensional normed spaces. *Proc. Amer. Math. Soc.*, 94: 445–449.

[1989] Pisier, G. *The volume of convex bodies and Banach space geometry.* Cambridge Tracts in Mathematics 94, Cambridge Univ. Press, 1989.