The generation of badly approximable pairs for communications via real interference alignment

11th IMA International Conference on Mathematics in Signal Processing, Birmingham, 2016-12-14 0945–1005

Lucinda Hadley (University of Lancaster) & Keith Briggs (BT TSO, Martlesham)

Abstract—Certain proposed coding schemes require sets of irrational numbers $(a_1, a_2, ..., a_n)$ which define linear forms. It is conjectured that the more badly approximable these linear forms, meaning the greater the positive lower bound of $q^n|q+p_1a_1+\cdots+p_na_n|$ for any choice of integers $(q, p_1, \ldots, p_n)$, the better the coding scheme. In contrast to classical one-dimensional Diophantine approximation theory ($n=1$), the situation for $n>1$ is full of unsolved problems, and it is not even known what the worst approximable pair is. The aim of this paper will be to present some purely numerical results which suggest some good candidates for bad pairs, and to demonstrate the performance of these pairs in a transmission protocol. For this we use an algorithm due to Vaughan Clarkson, but the software implementation requires some delicate treatment of floating-point arithmetic. This results in the first fully-rigorous implementation of an algorithm for finding the sequence of best approximants for a linear form $q+p_1a_1+p_2a_2$, and for the simultaneous rational approximation of two irrationals. Finally, we demonstrate the effect of using such linear forms on the error rate of our coding scheme.

1 Summary of the classical one-dimensional theory

We may measure the goodness of approximation of the rational number p/q to α by $c(\alpha,p,q)\equiv q|q\alpha-p|$. For each irrational α we know that there are infinitely many rationals p/q such that $|\alpha-p/q|<1/q^2$; that is, $c(\alpha,p,q)<1$. It is therefore of interest to ask how small one may make κ in $c(\alpha,p,q)<\kappa$ before this property fails to hold. The *approximation constant* of α is thus defined as $c(\alpha)\equiv \liminf_{q\to\infty}\min_p c(\alpha,p,q)$; or, introducing the notation $\boxdot\alpha$ for the distance from α to the nearest integer, $c(\alpha)=\liminf_{q\to\infty} q\,\boxdot q\alpha$.

Thus, numbers α with a large $c(\alpha)$ are hard to approximate by rationals. The *one-dimensional diophantine approximation constant* can now be defined as $c_1=\limsup_{\alpha\in\mathbb{R}} c(\alpha)$, and this is known to have the value $1/\sqrt{5}$. Otherwise expressed, this means that c_1 is the unique number such that for each $\epsilon>0$, $c(\alpha,p,q)<c_1+\epsilon$ has infinitely many rational solutions p/q for all α, whereas there is at least one α such that $c(\alpha,p,q)<c_1-\epsilon$ has only finitely many rational solutions.

2 Two-dimensional theory

We wish to simultaneously approximate a pair of irrationals (α_1,α_2) by a pair of rationals with common denominator. For a norm (radius function) f, we extend the meaning of the symbol $\boxdot$ by

$$\boxdot\boldsymbol{\alpha} \equiv \min_{\boldsymbol{p}\in\mathbb{Z}^2} f(|q\alpha_1-p_1|,|q\alpha_2-p_2|).$$

Now for

$$\boldsymbol{p}=(p_1,p_2)\in\mathbb{Z}^2, q\in\mathbb{Z}, \boldsymbol{\alpha}=(\alpha_1,\alpha_2)\in\mathbb{R}^2\setminus\mathbb{Q}^2,$$

let

$$\begin{aligned} c(\boldsymbol{\alpha},q) &= q\boxdot\boldsymbol{\alpha}^2, \\ c(\boldsymbol{\alpha}) &= \liminf_{q\to\infty} c(\boldsymbol{\alpha},q). \end{aligned}$$

The two-dimensional f-norm simultaneous diophantine approximation constant is then $c_2=\sup_{\boldsymbol{\alpha}} c(\boldsymbol{\alpha})$. Despite much work over the last few decades (Adams 1969, 1980; Cassels 1955; Cusick 1974, 1983; Kratz 1999; Szekeres 1984, 1985), the value of c_2 is unknown, though folklore suggests that its value is $2/7$. Nowak 1981 has shown that the value of c_2 is less than or equal to $\frac{64}{169}\approx 0.378698$. To study this question further (at least, numerically) we need an algorithm for finding all best approximations for a given $\boldsymbol{\alpha}$ up to a given denominator $q_{\max}$.

3 Two-dimensional algorithms

Our aim is to implement a practical algorithm for computing the sequence of best Diophantine approximations for two dual problems, given a pair of irrational numbers (α_1,α_2). This is done in order to estimate the approximation constant of the pair.

- Firstly, we have the simultaneous approximation problem; that is, to make the "radius" $r(|q\alpha_1-p_1|,|q\alpha_2-p_2|)$ small, where r is some norm on $\mathbb{R}^2$, while not making the "height" $h(q)\equiv q$ too big.
- Secondly, we have the problem of minimization of a linear form; that is, to make the radius

$$|q+\alpha_1 p_1+\alpha_2 p_2| \tag{1}$$

small, while not making the height $h(\alpha_1,\alpha_2)$ (measured by some norm h on $\mathbb{R}^2$) too big.

This was achieved, under some (relatively weak, and manageable) constraints on the functions r and h, by Clarkson (1997).

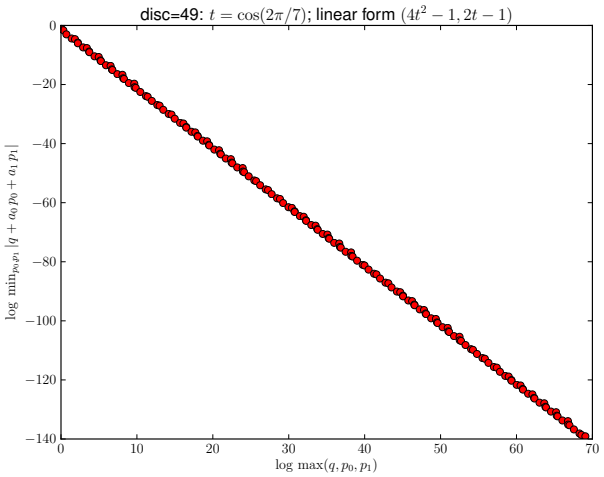

Fig. 1. Diophantine minimization of a linear form defined by a badly approximable irrational pair, plotted at at best approximation denominators.

3.1 The worst approximable pair

The algorithm allows an estimate of several properties of the irrational pair of number-theoretic interest: decrease of log norm (radius) with log denominator q; growth rate of the best approximation denominators $q_i^{1/i}$; the values $c(\boldsymbol{\alpha}, q) = q|\overline{\boldsymbol{\alpha}}|^2$ at best approximation denominators. The (uncomputable) value $c(\boldsymbol{\alpha})$ is the liminf of this as $q \to \infty$. The behaviour for the pair $(4t^2–1, 2t–1)$ with t=cos $(2\pi/7)$ is shown in Figure 1. Using other techniques, Briggs (2003) has shown that there exists a pair (α, β) with $c(\alpha, \beta) \approx$ 0.285710526941, and this value (very close to 2/7), is still the highest known.

The algorithms of Clarkson have several appealing features:

- They are designed for quite general approximation problems.
- They come with correctness proofs.
- All the real arithmetic is contained within one function L.
- They can be implemented with an "oracle" model for the computation of the irrational pair.
- The irrational pair is not mapped to a new one for subsequent steps, unlike on some other algorithms (which would make backtracking when increased precisiosn is needed very difficult).

4 Wireless communications

We now introduce the basics of wireless communications and explain the motivation for applying the theory in previous sections to the underlying design of certain wireless systems.

Our interest is in coding schemes equipped with a receive constellation, which functions as a key telling the receiver which waveform to produce for which symbol, and vice versa. Visually, it is a diagram containing 2^n points, each of which the transmitter assigns to a unique symbol of length n. The modulation of the carrier wave is determined by the co-ordinates of the point representing each symbol in the constellation. When the signal arrives at the receive antenna, it measures the voltage and frequency of the current generated and refers to its own constellation map to determine which symbol to produce from the wave form.

Noise distortion over the wireless channel means that variables are sometimes altered enough to result in an incorrect constellation point assignment upon receipt, so that some bits are decoded incorrectly. We seek to minimise this error rate by using constellations based on badly approximable linear forms. The key variables are the variance of the noise in the environment and the spacing of the points in the transmit and receive-constellations (Proakis 1995).

4.1 Model

For this paper we consider a generalised uplink multiple-input-single-output (MISO) system that supports m users, and is subject to flat fading. We assume there is a single antenna in each user's device, each with its own channel link to a base station, and that the m transmitted data streams are independent. We model a data stream as a vector S of randomly assigned bits and the noise as a vector with Gaussian distributed entries having 0 mean and variable variance v, which we add pointwise to S.

Table 1 shows the arrival points of symbols transmitted and distorted using our model, for a constellation of just four points on the real line. Notice that the bit error rate (BER) increases as the noise variance increases, but decreases when we increase the space between constellation points.

Definition 4.1: We define a constellation $\mathcal{U}_m$ on the real line as the set of all linear combinations u_i of the basis elements $\{\alpha_0, \alpha_1, ..., \alpha_{m-1}\}$ $(m \in \mathbb{N})$ over the set $\mathcal{S} = \{0, 1, ..., 2^n - 1\}$ where

$$u_i = q + \alpha_1 p_{i1} + ... + \alpha_{(m-1)} p_{i(m-1)} \;\big|\; q, p_{ik} \in \mathcal{S}.$$

If we set m=3, this constellation contains points in the linear form given in Equation (1). This type of constellation is used in Motahari et al. 2010. and we may denote the minimum separation of any two distinct points $u_i, u_j \in \mathcal{U}_m$ as a function $d_{\min}: \mathbb{R}^2 \mapsto \mathbb{R}$ of the elements $(\alpha_1, \alpha_2, ..., \alpha_{m-1})$:

$$d_{\min}(\alpha_1, \alpha_2, ..., \alpha_{m-1}) = \min_{i \neq j} |u_i - u_j|.$$

Maximising the minimum separation reduces error rate because it means that a distorted signal is less likely to be mapped to the wrong constellation point.

5 Investigation

In this section, we carry out a new investigation into the effect the values α_1 and α_2 have on the BER of the constellation $\mathcal{U}_m$, and test the hypothesis:

H 1: $\mathcal{U}_m$ has a greater minimum separation of points for simultaneously badly approximable values of α_k.

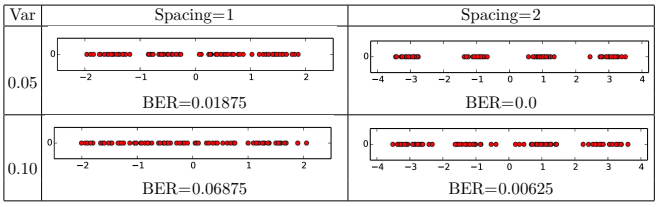

TABLE 1
Effect of changing variance and spacing.

5.1 One dimension

By the results in Section 1, if a simultaneously badly approximable pair produces better constellations in two dimensions, it should follow that $\varphi=\frac{1+\sqrt{5}}{2}$, the golden ratio, produces an optimal constellation in one dimension. Therefore, we start by testing the one-dimensional constellation $\mathcal{U}_1$, in which our rationally independent basis has two elements, 1 and α and our constellation points are $\mathcal{U}_1 \ni u_i = q+\alpha_1 p_{i1}$, where $q, p_{i1} \in \{0, 1, ..., 2^n\}$.

H 2: The more badly approximable the value of α_1, the more evenly spaced the constellation $\mathcal{U}_1$.

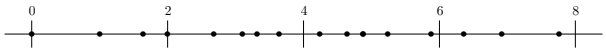

Fig. 2. Constellation for 2-bit symbols over rational basis $\{1, \varphi\}$.

Figure 2 shows a constellation of the form given in Hypothesis 2 with $n=2$ and $\alpha_1=\varphi$. In order to disprove Hypothesis 2, we need only show that there is some irrational $\alpha_1 \neq \varphi$ for which $d_{\min}(\alpha_1) > d_{\min}(\varphi)$ for some symbol length n. When $n=4$ we find that $d_{\min}(\varphi) \approx 0.00142 < 0.00228 \approx d_{\min}(\pi)$. Since φ is the most badly approximable irrational number, and since, in particular, π is less badly approximable, this disproves Hypothesis 2. In fact, we find that different values of α_1 maximize $d_{\min}(\alpha_1)$ for different symbol lengths n. For example, when $n=3$ we have $d_{\min}(\varphi) > d_{\min}(\pi)$, in contrast to the case we have just demonstrated for $n=4$, and we conclude that the optimum value for α_1 depends on n.

To investigate the impact of changing α_1, on the constellation spacing, we consider the most basic case where $n=1$, we have $2^{2n}=4$ constellation points and the possible linear combinations are given by $0, 1, \alpha_1$ and α_1+1. Given our definition of minimum distance, the optimally spaced constellation in this instance is given by $\alpha_1=\frac{1}{2}$, since this value will produce an evenly spaced constellation.

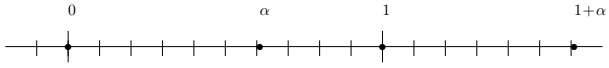

Fig. 3. Constellation with $\alpha_1=\frac{1}{\varphi}$ and $n=1$.

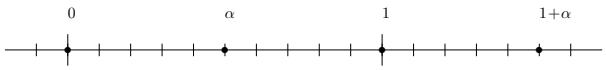

Fig. 4. Constellation with $\alpha_1=\frac{1}{2}$ and $n=1$.

In fact, by taking $\alpha_1=\frac{1}{2^n}$ the resulting constellation of points is optimally spaced for each n giving a generalised constellation of the form in Figure 5.

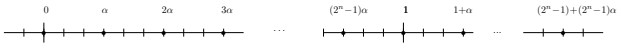

Fig. 5. Constellation for any n with $\alpha_1=\frac{1}{2^n}$.

Table 2, demonstrates explicitly the preferability of $\alpha_1=\frac{1}{2^n}$ to $\alpha_1=\varphi$ by picturing the relevant (scaled) constellations side by side for some values of n and comparing the minimum distance between points.

The reason our hypothesis fails is that, in practice, we do not allow the linear combinations to be taken over the entire range of integers but restrict it to the finite set $\{0, 1, ..., 2^n-1\}$. In fact, the basis $\{1, \frac{1}{2^n}\}$ *is* rationally independent over this bounded set, which is why we are able to use a rational number for α_1. Therefore, we cannot improve upon constellation 5.1 using the theory of badly approximable numbers.

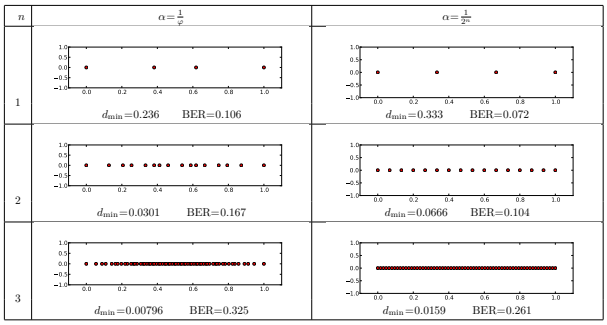

TABLE 2
Comparison of constellations with $\alpha=\varphi$ and $\alpha=\frac{1}{2^n}$.

5.2 Multiple dimensions

As we would expect, the same problem occurs in two dimensions. In this case, our most basic constellation consists of points $u_i = q+\alpha_1 q_{i1}+\alpha_2 q_{i2}$ such that $p, q_{ik} \in \{0, 1\}$. Using the candidates for the worst approximable pair, $\alpha_1=4t^2-1$ and $\alpha_2=2t-1$ for $t=\cos\left(\frac{2\pi}{7}\right)$, put forward in Section 3.1, we obtain the constellation in Figure 6.

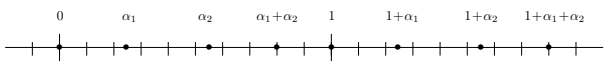

Fig. 6. Constellations with $\alpha_1=4t^2-1$ and $\alpha_2=2t-1$ for $t=\cos\left(\frac{2\pi}{7}\right)$.

As before, however, we can improve on this by defining α_1 and α_2 in terms of n. If we let $\alpha_1 = \frac{1}{2^n}$ and $\alpha_2 = \frac{\alpha_1}{2^2} = \frac{1}{2^{2n}}$ we get an evenly spaced constellation containing 2^{3n} points, so that the linear combinations containing α_2 as a component produce a point in the centre of each of the spaces in Figure 4. In the general case, the points for which the coefficient of α_2 is non-zero 'fill up' the spaces in the corresponding one-dimensional case so that the generalised constellation is given by figure 7.

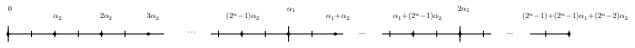

Fig. 7. Constellation for any n with $\alpha_1 = \frac{1}{2^n}$ and $\alpha_2 = \frac{1}{2^{2n}}$.

In fact we can extend this reasoning beyond the 2-dimensional case. Suppose we have a constellation of the form

$$\mathcal{U}_m \ni u_i = q + \alpha_1 p_{i1} + \alpha_2 p_{i2} + ... + \alpha_m p_{im}$$

such that $m \in \mathbb{N}$, $p_{ik} \in \{0, 1, ..., 2^n - 1\}$ and the α_k are rationally independent for $k \in \{0, 1, ..., m\}$. Then we have m dimensions, and if we define $\alpha_k = \frac{1}{2^{kn}}$ for each $k \in \{1, ..., m\}$, we obtain an evenly spaced constellation, where the points with non-zero coefficients for α_{k+1} are evenly spaced to fill the gaps between points with non-zero coefficients α_k and zero coefficients for α_{k+1}.

We may also calculate the minimum distance in any such constellation, since it is given by the smallest α_k as is demonstrated in Figures 5 and 7. Once we scale this distance to account for range, we have, for a constellation X of linear combinations of the basis $\{1, \alpha_1, ..., \alpha_m\}$ over the set of symbol representations $\{0, 1, 2, ...2^n\}$:

$$d_{\min}(X) = \frac{1}{2^{(m+1)n}(2^n - 1)(1 + \alpha_1 + ... + \alpha_m)},$$

which depends only on n and m.

6 Conclusion

Our research has extended the search for badly approximable numbers into two dimensions and given candidates for badly approximable pairs $\alpha = (\alpha_1, \alpha_2)$. We have shown that using badly approximable numbers, or badly approximable pairs of numbers as basis elements for one and two-dimensional linear combination generated constellations respectively, has no advantage over using regular even spacing, which can be achieved easily as is detailed above.

There are several areas for further investigation, for instance, we have focussed on maximising minimum distance, however, assuming a uniform distribution, perhaps an ideal constellation should make it equally likely for any symbol to be decoded correctly. In this case, having points spaced closer together at the ends and more sparsely in the middle of the range would be more appropriate.

Another point to consider is that the set of symbols to be transmitted may not be uniformly distributed. In this case, a constellation with unevenly spaced points with varying probabilities of being received in error could be intelligently assigned in order to reduce the BER of the system. It would be interesting to discover the optimal constellation for a given probability distribution, and this might be an opportunity to use the linear combinatory approach.

We have seen that Diophantine Approximation, despite being an area known to mathematicians for hundreds of years, is still producing new results. Further examples of applications can be found in the areas of physics, the geometry of numbers, room acoustics and cryptography, which can be read about in Schroeder 2009, along with many other applications of more generalised number theory.

References

Adams, W. W. (1969). "Simultaneous Diophantine Approximations and Cubic Irrationals". In: *Pacific J. Math.* 30, pp. 1–14.

– (1980). "The best two-dimensional Diophantine approximation constant for cubic irrationals". In: *Pacific J. Math.* 91, pp. 29–30.

Briggs, Keith (2003). "Some explicit badly approximable pairs". In: *Journal of Number Theory* 103, pp. 71–76.

Cassels, J. W. S. (1955). "Simultaneous Diophantine Approximation". In: *J. Lond. Math. Soc.* 30, pp. 119–121.

Clarkson, I. Vaughan L. (1997). "Approximation of Linear Forms by Lattice Points with Applications to Signal Processing". PhD thesis. The Australian National University.

Cusick, T. W. (1974). "The two-dimensional Diophantine Approximation Constant". In: *Monatshefte für Mathematik* 78, pp. 297–304.

– (1983). "The two-dimensional Diophantine Approximation Constant. II". In: *Pacific J. Math.* 105, pp. 53–67.

Kratz, Werner (1999). "On optimal constants for best two-dimensional simultaneous Diophantine approximations". In: *Monatshefte für Mathematik* 128, pp. 99–110.

Motahari, Abolfazl S. et al. (2010). "Real Interference Alignment". In: *CoRR* abs/1001.3403.

Nowak, W. G. (1981). "A note on simultaneous Diophantine approximation". In: *Manuscripta Math.* 36. MR 83a:10062, pp. 33–46.

Proakis, John G (1995). *Digital communications*. McGraw-Hill, New York.

Schroeder, Manfred (2009). *Number theory in science and communication: with applications in cryptography, physics, digital information, computing, and self-similarity*. Vol. 7. Springer.

Szekeres, G. (1984). "The N-dimensional approximation constant". In: *Bull. Austral. Math. Soc.* 29, pp. 119–125.

– (1985). "Computer examination of the 2-dimensional simultaneous approximation constant". In: *Ars Combinatoria* 19A, pp. 237–243.