Mathematics of Signal Design for Communication Systems and Szemerédi's and Green-Tao's Theorems

Holger Boche
joint work with Ezra Tampubolon

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

Mathematisches Kolloquium
Fachgruppe Mathematik, RWTH Aachen, Aachen – January 22, 2016

Motivation – Orthogonal Transmission Scheme

- Orthogonal transmission scheme:

$$s(t) = \sum_{k=1}^{N} a_k \phi_k(t), \quad t \in [0, T_s].$$

  - N – Number of carriers/wavefunctions,
  - T_s – Duration of a communication symbol (w.l.o.g. $T_s = 1$),
  - $\{\phi_n\}_{n=1}^{N}$ – (Bounded) Orthonormal system (ONS) in $L^2([0, T_s])$,
  - $\{a_k\}_{k=1}^{N}$ – Transmit data.
- Orthogonal transmission scheme plays an important role for present -, and future communications standards, e.g.:
  - Orthogonal frequency division multiplexing (OFDM):

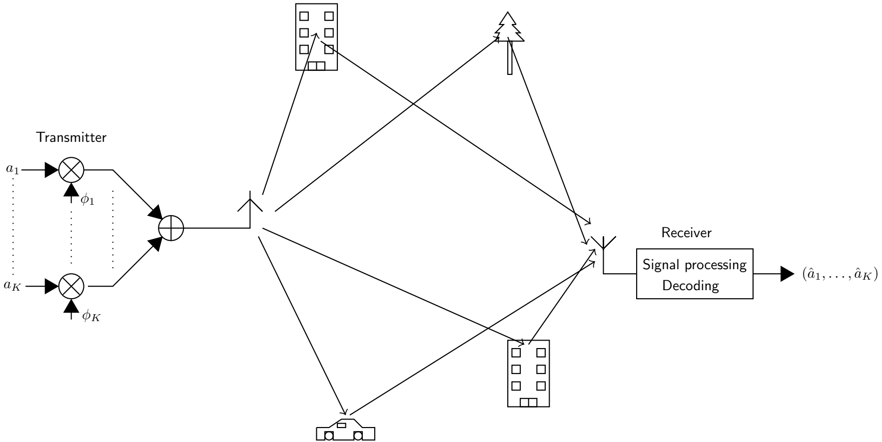
$$\phi_n(\cdot) = e^{i2\pi(n-1)(\cdot)} =: e_{n-1}(\cdot).$$

    Applications: DSL, IEEE 802.11, DVB-T, LTE, and LTE-advanced/4G.
  - Code division multiple access (CDMA):

$$\phi_n - \text{Walsh function (Defined later)}.$$

    Applications: 3G, UMTS, GPS, and Galileo.

Orthogonal Transmission Scheme - Sketch



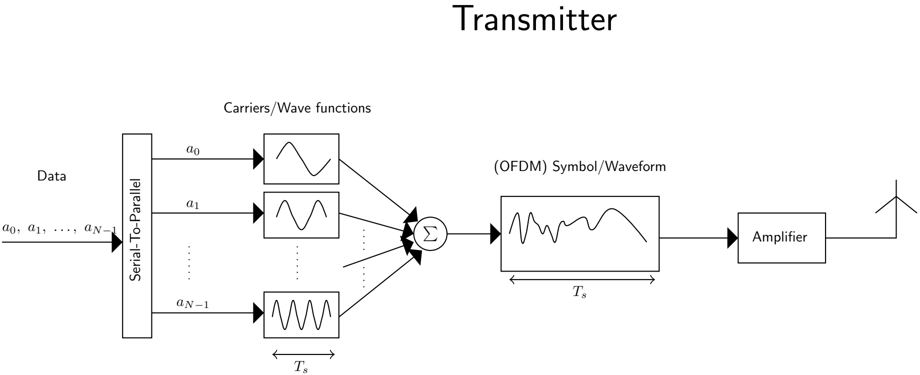
Motivation – Dynamics of Orthogonal Transmission Scheme

- Major drawback of orthogonal transmission scheme is its high dynamics, which is measured by the so-called Peak-to-Average-Power-Ratio (PAPR):

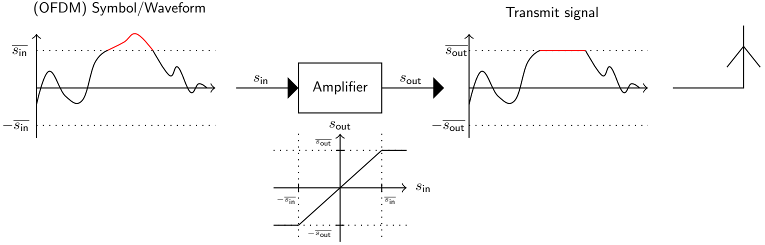
$$\mathrm{PAPR}(\{\phi_n\}_{n=1}^N, \mathbf{a}) := \frac{\left\| \sum_{k=1}^N a_k \phi_k \right\|_{L^\infty([0,1])}}{\left\| \sum_{k=1}^N a_k \phi_k \right\|_{L^2([0,1])}} = \operatorname*{ess\,sup}_{t\in[0,1]} \frac{\left| \sum_{k=1}^\infty a_k \phi_k(t) \right|}{\|\mathbf{a}\|_{l^2(\mathbb{N})}},$$

  for a sequence/data $\mathbf{a}$ in $\mathbb{C}$.
- High PAPR value of orthogonal transmission scheme have in particular negative impacts to the reliability -, energy efficiency -, and cost efficiency of a communications system.

Example of an Orthogonal Transmission Scheme - OFDM



Drawback of OFDM - The Effect of Clipping



- ▷ Occurence of clipping in case that the waveforms possess high dynamics, and the linear range of the used amplifier is not sufficiently large.
  - ↯ Out-of-band radiation of the transmit signal.
  - ⇒ Need for costly analog filter, to ensure that the transmit signal lies within a regulated frequency mask.
  - ↯ Alteration of the transmit signal.
  - ⇒ Error occurs!
- ↯ Amplifier with high linear range is expensive, and might cause high maintenance cost.

Drawback of OFDM

- Reports of consulting firms: 2% of global CO_2 emissions are attributable to the use of information and communication technology, which is comparable to the CO_2 emissions due to avionic activities.
- Energy cost of network operation can even make up to 50% of the total operational cost.

B. Boccaletti, M. Löffler, and J. Oppenheim,
How IT can cut carbon emmisions.
McKinsey Quarterly, October (2008)

Parliamentary Office of Science and Technology (UK),
ICT and CO 2 emmissions.
Postnote, December (2008)

Motivation – High Dynamics of Orthogonal Transmission Scheme

- PAPR values of order $\sqrt{N}$ can occur for any orthonormal system $\{\phi_n\}_{n\in[N]}$:

There exists a sequence $\mathbf{a} \in l^2([N])$, *with* $\|\mathbf{a}\|_{l^2([N])} = 1$, *such that:*

$$\sqrt{N} \leq \mathrm{PAPR}(\{\phi_k\}_{k\in[N]}, \mathbf{a}).$$

- For instance, there are up to 2048 wave functions used for the downlink communication in the LTE standard (OFDM).

$\Rightarrow$ Important to control the PAPR behaviour of orthogonal transmission scheme!

H. Boche and V. Pohl,
Signal representation and approximation - fundamental limits.
European Trans. Telecomm. (ETT) **5** (2007), 445–456.

Motivation – Tone Reservation method

- ▷ Tone reservation (Tellado and Cioffi):
  - Reserve one subset of functions of an ONS for carrying the information-bearing coefficients.
  - Determine coefficients for the remaining tones, s.t. the combined sum has a small peak value, below a certain desired threshold value.
- ▷ Tone reservation method is canonical, since the only knowledge needed by receiver is the (fixed) location of information-bearing coefficients.
- ▷ **Our goal**: To show that the tone reservation is not applicable for arbitrary threshold value.

J. Tellado, **Peak to average power reduction for multicarrier modulation,** *Ph.D. Thesis Stanford University*, (1999)

J. Tellado and J.M. Ciofi, **Peak to average power ratio reduction,** *U.S. patent application Ser.*, No. 09/062, 867, Apr. 20, 1998

J. Tellado and J.M. Ciofi, **Efficient algorithms for reducing PAR in multicarrier systems,** *Proc. IEEE ISIT* (1998), 191.

„Ich behaupte aber, daß in jeder besonderen Naturlehre nur so viel eigentliche Wissenschaft angetroffen werden könne, als darin Mathematik anzutreffen ist.“

— Immanuel Kant, Metaphysische Anfangsgründe der Naturwissenschaft (1787)

Outline

Outline

1. PAPR Reduction Problem

2. Conditions for the Solvability of the PAPR Reduction Problem
   - Necessary Condition
   - Sufficient Condition

3. Solvability of PAPR Reduction Problem for OFDM – Arithmetic Progressions
   - Szemerédi Theorem on Arithmetic Progressions, Green-Tao's -, and Conlon-Gower's Theorem for Sparse Sets
   - Application of the Szemerédi Thm. to the PAPR Problem for OFDM

4. Solvability of PAPR Reduction Problem for CDMA – Perfect Walsh Sum
   - Perfect Walsh Sum (PWS)
   - Existence of PWS in an Index Set
   - Necessary Condition for the PAPR reduction problem for CDMA case - PWS
   - Asymptotic Theorems for PWS

5. Summary and Conclusions

PAPR Reduction Problem - Formulation

- Given a desired threshold constant $C_{\mathsf{Ex}} > 0$. We aim to analyze, whether the tone reservation method is applicable in this case for a certain ONS.

Definition 1.1 (PAPR Reduction Problem)

Given $\mathcal{K} \subset \mathbb{N}$. Let $\{\phi_n\}_{n\in\mathcal{K}}$ be an ONS, and $\mathcal{I} \subset \mathcal{K}$. We say the PAPR reduction problem is solvable for the pair $(\{\phi_n\}_{n\in\mathcal{K}}, \mathcal{I})$ with constant $C_{\mathsf{Ex}} > 0$, if for every $\mathbf{a} \in l^2(\mathcal{I})$, there exists $\mathbf{b} \in l^2(\mathcal{I}^c)$ (the complementation is w.r.t. $\mathcal{K}$), satisfying $\|\mathbf{b}\|_{l^2(\mathcal{I}^c)} \leq C_{\mathsf{Ex}} \|\mathbf{a}\|_{l^2(\mathcal{I})}$, for which it holds:

$$\operatorname*{ess\,sup}_{t\in[0,1]} \left| \sum_{k\in\mathcal{I}} a_k\phi_k(t) + \sum_{k\in\mathcal{I}^c} b_k\phi_k(t) \right| \leq C_{\mathsf{Ex}} \|\mathbf{a}\|_{l^2(\mathcal{I})} .$$

We call $\mathcal{I}$ the <u>information set</u>, $\mathcal{I}^c$ the <u>compensation set</u>, C_{Ex} the <u>extension constant</u>.

PAPR Reduction Problem - Remarks

- Mostly: $\mathcal{K} = \mathbb{N}$. Thus, the compensation set is allowed to be infinite. In particular, we aim to show, that the PAPR reduction problem is not solvable for arbitrary extension constant.
  $\Rightarrow$ Restriction in the case that the compensation set is finite.
- PAPR reduction Problem can also be formulated by means of an extension operator (not necessarily linear!):

$$\mathrm{E}_{\mathcal{I}} : l^2(\mathcal{I}) \to L^\infty([0,1]), \quad \mathbf{a} \mapsto \sum_{k\in\mathcal{I}} a_k \phi_k + \sum_{k\in\mathcal{I}^c} b_k \phi_k,$$

  for suitable coefficients $\mathbf{b}$ (depend on the choice of $\mathbf{a}$!):

Given $\mathcal{K} \subset \mathbb{N}$. Let $\{\phi_n\}_{n\in\mathcal{K}}$ be an ONS, and $\mathcal{I} \subset \mathcal{K}$. The PAPR reduction problem is solvable for the pair $(\{\phi_n\}_{n\in\mathcal{K}}, \mathcal{I})$ with constant $C_{\mathsf{Ex}} > 0$, if there exists an extension operator, for which it holds:

$$\|\mathrm{E}_{\mathcal{I}}\mathbf{a}\|_{L^\infty([0,1])} \le C_{\mathsf{Ex}} \|\mathbf{a}\|_{l^2(\mathcal{I})} .$$

Outline

Necessary and Sufficient Conditions - Essential Subspaces

- **Plan**: Derive (especially necessary) conditions for the solvability of PAPR reduction problem, suitable for our approach to show the limitation of the PAPR reduction problem
  The following subspaces of $L^1([0,1])$ plays an important role:

Definition 2.1

For an $\mathcal{I} \subset \mathbb{N}$, and an ONS $\{\phi_n\}_{n\in\mathbb{N}}$, we define the following subspaces of $L^1([0,1])$:

$$\mathfrak{F}^1(\mathcal{I}) := \left\{ f \in L^1([0,1]) : \; f = \sum_{k\in\mathcal{I}} a_k \phi_k, \; \text{for a } \{a_k\}_{k\in\mathcal{I}} \text{ in } \mathbb{C} \right\}$$

$$\mathfrak{F}_c^1(\mathcal{I}) := \left\{ f \in L^1([0,1]) : \; f = \sum_{k\in\mathcal{I}} a_k \phi_k, \; a_k \neq 0, \; \text{for finitely many } k \in \mathcal{I} \right\}$$

Necessary and Sufficient Conditions - Essential Subspaces

- **Basic properties of $\mathfrak{F}^1(\mathcal{I})$ and $\mathfrak{F}_c^1(\mathcal{I})$:**
  - $\mathfrak{F}^1(\mathcal{I})$ is a closed subspace of $L^1([0,1])$.
  - $\mathfrak{F}_c^1(\mathcal{I})$ is a dense subspace of $\mathfrak{F}^1(\mathcal{I})$.
- It turns out that the solvability of the PAPR reduction problem is connected to the Embedding problem of $\mathfrak{F}^1(\mathcal{I})$ into $L^2(\mathcal{I})$.

Necessary Condition

Theorem 2.2 (B. and Farell)

Let $\{\phi_n\}_{n\in\mathbb{N}}$ *be a complete ONS in* $L^2([0,1])$. *Given a subset* $\mathcal{I}\subset\mathbb{N}$ *and a constant* $C_{\mathsf{Ex}}>0$. *Assume that the PAPR reduction problem is solvable for* $(\{\phi_n\}_{n\in\mathbb{N}},\mathcal{I})$ *with extension constant* C_{Ex}. *Then:*

$$\|f\|_{L^2([0,1])}\leq C_{\mathsf{Ex}}\|f\|_{L^1([0,1])}, \quad \forall f\in\mathfrak{F}^1(\mathcal{I}).$$

H. Boche and B. Farell,
On the Peak-to-Average Power Ratio Reduction Problem for Orthogonal Transmission Schemes.
Internet Mathematics, **9** (2–3) (2013), 265–296

Necessary Condition - Sketch of Proof

- By density arguments, it is sufficient to show the inequality for all $f \in \mathfrak{F}_c^1(\mathcal{I})$.
- By the assumption of the solv. of the PAPR red. prob., and the Parseval's id., for arb. $f \in \mathfrak{F}_c^1(\mathcal{I})$, $f = \sum_{k\in\mathcal{I}} c_k\phi_k$, and $\mathbf{a} \in l^2(\mathcal{I})$, one can obtain the following equality:

$$\left|\sum_{k\in\mathcal{I}} c_k\overline{a_k}\right| = \left|\sum_{k\in\mathcal{I}} c_k\overline{a_k} + \sum_{k\in\mathcal{I}^c} c_k\overline{a_k}\right| = \left|\int_0^1 f(t)\overline{(\mathrm{E}_{\mathcal{I}}(\mathbf{a}))(t)}\mathrm{d}t\right|,$$

  where $c_k := 0$, $\forall k \in \mathcal{I}^c$, and a_k, $k \in \mathcal{I}^c$, are the coeff. determined by a suitable extension operator $\mathrm{E}_{\mathcal{I}}$.
- Parseval's identity, and the Hölder's inequality give further hints:

$$\begin{aligned}\left|\sum_{k\in\mathcal{I}} c_k\overline{a_k}\right| &= \left|\int_0^1 f(t)\overline{(\mathrm{E}_{\mathcal{I}}(\mathbf{a}))(t)}\right| \leq \|f\|_{L^1[0,1]} \|\mathrm{E}_{\mathcal{I}}(\mathbf{a})\|_{L^\infty([0,1])} \\ &\leq C_{\mathsf{Ex}} \|f\|_{L^1([0,1])} \|\mathbf{a}\|_{l^2(\mathcal{I})}.\end{aligned}$$

- Finally, by setting $\mathbf{a} = \mathbf{c}$, and Parseval's identity, the desired statement can be obtained.

Sufficient Condition

Theorem 2.3 (B. and Farell)

Let $\{\phi_n\}_{n\in\mathbb{N}}$ *be a complete ONS for* $L^2([0,1])$*, and let be* $\mathcal{I} \subset \mathbb{N}$*, and* $C_{\mathsf{Ex}} > 0$*. If the following condition is fulfilled:*

$$\|f\|_{L^2([0,1])} \le C_{\mathsf{Ex}} \|f\|_{L^1([0,1])}, \quad \forall f \in \mathfrak{F}^1(\mathcal{I}),$$

then the PAPR reduction problem is solvable for $(\{\phi_n\}_{n\in\mathbb{N}}, \mathcal{I})$ *with extension constant* C_{Ex}*.*

Main ingredients of the proof:

- Hahn-Banach Theorem.
- $L^\infty([0,1])$ is the dual space of $L^1([0,1])$/ Representation of functionals on $L^1([0,1])$.

H. Boche and B. Farell,
On the Peak-to-Average Power Ratio Reduction Problem for Orthogonal Transmission Schemes.
Internet Mathematics, **9** (2–3) (2013), 265–296

Outline

Solvability of PAPR Problem - OFDM

- Recall: The solvability of PAPR reduction problem is connected with embedding problem of a closed subspace $\mathfrak{F}^1(\mathcal{I})$ of $L^1([0,1])$ into $L^2([0,1])$.
- Explicitly: For sake that the PAPR reduction problem is solvable for $(\{\phi_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with a given extension constant $C_{\mathsf{Ex}} > 0$, it is necessary that the following inequality holds:

$$\|f\|_{L^2([0,1])} \leq C_{\mathsf{Ex}} \|f\|_{L^1([0,1])}, \quad \forall f \in \mathfrak{F}^1(\mathcal{I}), \tag{1}$$

$\Rightarrow$ To show that the PAPR reduction problem is not solvable for $(\{\phi_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with a given extension constant $C_{\mathsf{Ex}} > 0$, it is sufficient to search functions in $\mathfrak{F}^1(\mathcal{I})$, for which (1) does not hold.

- **Later**: The existence of such functions is connected to the existence of certain combinatorials objects in the information set $\mathcal{I}$, viz.:
  - Arithmetic progression in the OFDM case,
  - Perfect Walsh sum in the CDMA case.

Szemerédi Theorem on Arithmetic Progressions

Definition 3.1 (Arithmetic Progression)

Let be $m \in \mathbb{N}$. An arithmetic progression of length m is defined as a subset of $\mathbb{Z}$, which has the form:

$$\{a, a+d, a+2d, \ldots, a+(m-1)d\},$$

for some integer a and some positive integer d.

- ▷ For sets with specific structures, such as sum sets $\mathcal{A}+\mathcal{A}$, $\mathcal{A}+\mathcal{A}+\mathcal{A}$, $2\mathcal{A}-2\mathcal{A}$, for a $\mathcal{A} \subset \mathbb{N}$, there are some results concerning to the existence of arithmetic progressions within those sets.
- $\lightning$ Those results require some insights into the structure of $\mathcal{A}$
- ▷ Is it possible to give a statement on the existence of arithmetic progression(s) within a set $\mathcal{A}$, only by knowing the size of $\mathcal{A}$?

Szemerédi Theorem on Arithmetic Progressions

Definition 3.2 ((δ, m)-Szemerédi Set)

Let $\mathcal{I}$ be a set of integers, $\delta \in (0,1)$, and $m \in \mathbb{N}$. The set $\mathcal{I}$ is said to be (δ, m)-Szemerédi, if every subset of $\mathcal{I}$ of cardinality at least $\delta\,|\mathcal{I}|$ contains an arithmetic progression of length m.

Theorem 3.3 (Széméredi Theorem)

For any $m \in \mathbb{N}$, and any $\delta \in (0,1)$, there exists $N_{Sz} \in \mathbb{N}$, which depends on m and δ, s.t. for all $N \geq N_{Sz}$, $[N]$ is (δ, m)-Szemerédi.

E. Szemerédi,
On sets of integers containing no k elements in arithmetic progressions.
Acta Arith., **27** (1975), 199–245.

Szemerédi Theorem - Historical Remarks

- The case $m = 3$ was established in 1953 by Klaus Roth (mentioned in his Fields medal citation in 1958).
- The case $m = 4$ was established in 1969 by Endre Szemerédi.
- The case $m \in \mathbb{N}$ was proven in 1975, also by Szemerdi (mentioned in his Abel prize citation in 2012).
  Erdös: "a masterpiece of combinatorial reasoning".
- Several alternative proof, e.g. by Timothy Gowers for $m = 4$ (mentioned in his Fields medal citation in 1998) and generally for $m \in \mathbb{N}$.

K. Roth, **On certain sets of integers.** *Journal of the London Mathematical Society*, **28** (1953), 104-109

E. Szemerédi, **On sets of integers containing no four elements in arithmetic progression.** *Acta Math. Acad. Sci. Hung.*, **20** (1969), 89 – 104

E. Szemerédi, **on sets of integers containing no k elements in arithmetic progression.** *Acta Arithmetica*, **27** (1975).

W. T. Gowers, **A New Proof of Szemerdi's Theorem for Arithmetic Progressions of Length Four.** *Geom. Funct. Anal.*, **8** (1998), 529 – 551.

W. T. Gowers, **A New Proof of Szemerdi's Theorem.** *Geom. Funct. Anal.*, **11** (2001), 465–588.

Szemerédi Theorem - Asymptotic Case

- For asymptotic case, Szemerédi Thm. is somehow unsatisfying. It only ensures the existence of arithmetic progressions of arbitrary length for subsets $\mathcal{A}$ of $\mathbb{N}$ with positive upper density, i.e.:

The set $\mathcal{A} \subset \mathbb{N}$ contains arithmetic progressions of arbitrary length if:

$$\limsup_{N\to\infty}(|\mathcal{A} \cap [N]| / N) > 0.$$

- A tightening of the Szemerédi is due to Green and Tao. They prove the existence of a subset $\mathcal{A}$ of $\mathbb{N}$ with density 0, i.e. $\lim_{n\to\infty}(|\mathcal{A} \cap [N]| / N) = 0$, containing arithmetic progressions of arbitrary length:

Theorem 3.4 (Green and Tao)

The set of prime numbers $\mathcal{P}$ contains arithmetic progressions of arbitrary length.

B. Green and T. Tao,
The primes contain arbitrarily long arithmetic progressions.
Annals of Mathematics **167** (2008), 481–547.

Szemerédi Theorem - Asymptotic Case and Probabilistic Case

- Another asymptotic tightening of Szemerédi Thm. is the following:

Theorem 3.5 (Conlon, Gowers)

Given $\delta > 0$, and a natural number $m \in \mathbb{N}$. There exists a constant $C > 0$, s.t.:

$$\lim_{N\to\infty} \mathbb{P}([N]_p \textit{ is } (\delta, m)\textit{-Szemerédi}) = 1, \quad \textit{if } p > CN^{\frac{-1}{(m-1)}}.$$

- Above Thm. ensures the existence of a sequence $\{p_N\}$ in $(0,1)$ tending to 0, for which:

$$\lim_{N\to\infty} \mathbb{P}([N]_{p_N} \text{ is } (\delta, m)\text{-Szemerédi}) = 1.$$

- In particular, the sets constructed by means $\{p_N\}_{N\in\mathbb{N}}$ has density zero.

D. Conlon and W. T. Gowers,
Combinatorial theorems in sparse random sets.
arXiv:1011.4301, (2011).

Szemerédi Theorem - Asymptotic case

- Given a subset $\mathcal{A}$ of $\mathbb{N}$, which is not too small (but possibly: $\mathcal{A}$ has density 0 in $\mathbb{N}$). Is one able to guarantee the existence of arithmetic progressions of arbitrary length within this set?

Erdös Conjecture on Arithmetic Progressions

Let $\mathcal{A}$ be a set of positive integers s.t. $\sum_{n\in\mathcal{A}} 1/n = \infty$. Then $\mathcal{A}$ contains an arbitrarily long arithmetic progressions.

- Erdös Conjecture on arithmetic progressions remain unsettled.
  It is even not known, whether $\mathcal{A}$ must contain arithmetic progressions of length 3.
- A set which fulfills the requirement of above conjecture, and contain an arbitrarily long arithmetic progressions: The set of prime numbers.

P. Erdös and R. L. Graham,
Old and New Problems and Results in Combinatorial Number Theory.
L'Enseignement Mathématique Université de Genève, **28** (1980).

Solvability of PAPR reduction problem & Arithmetic Progressions

Lemma 3.6

Let be $\mathcal{I} \subset \mathbb{N}$. Assume that there exists an arithmetic progression of length m in $\mathcal{I}$. Then, if the PAPR reduction problem is solvable for $(\{e_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with a given extension constant $C_{Ex} > 0$, it follows:

$$C_{Ex} > \frac{\sqrt{m}}{\frac{4}{\pi^2}\log\left(\frac{m}{2}\right) + C},$$

for an absolute constant $C > 0$.

Sketch of Proof:

- ▷ Consider the signal $f = \sum_{k=0}^{m-1} \frac{1}{\sqrt{m}} e_{a+dk} \in \mathfrak{F}^1(\mathcal{I})$, for some $a, d \in \mathbb{N}$.
- ▷ By Parseval's inequality, and usual bound for Dirichlet kernel, we have:

$$\|f\|_{L^2([0,1])} = 1, \quad \|f\|_{L^1([0,1])} < \frac{\frac{4}{\pi^2}\log\left(\frac{m}{2}\right) + C}{\sqrt{m}},$$

  for an absolute constant $C > 0$ (for instance: $C = 5 + \frac{2}{24-\pi^2}$).
- ▷ Necess. cond. for the solv. of PAPR reduction prob. gives the remaining.

Solvability of PAPR reduction problem & Arithmetic Progressions

Theorem 3.7

Given $\delta \in (0,1)$ *and* $m \in \mathbb{N}$, *then there exists an* $N_{Sz} \in \mathbb{N}$, *depending on* δ *and* m, *s.t. for all* $N \geq N_{Sz}$, *the following holds:*
If the PAPR reduction problem is solvable for $(\{e_n\}_{n\in\mathbb{N}}, \mathcal{I})$ *with* $C_{Ex} > 0$, *where* $\mathcal{I} \subset [N]$, *with* $|\mathcal{I}| \geq \delta N$, *then:*

$$C_{Ex} > \frac{\sqrt{m}}{\frac{4}{\pi^2}\log\left(\frac{m}{2}\right) + C}, \tag{2}$$

for an absolute constant $C > 0$.

- **Proof ingredients**: Previous Lemma and Szemerédi Thm.
- Above Thm. asserts, that there is a restriction to the size of the information set such that the PAPR reduction problem is solvable.

Asymptotic Tightenings of Thm. 3.7

- By Green and Tao's Thm.:

There exists a set $\mathcal{A}$ (the set of prime numbers) of density 0 in $\mathbb{N}$, s.t. for every $C_{\mathit{Ex}} > 0$, there exists $n_0 \in \mathbb{N}$, s.t. the PAPR reduction problem is not solvable for $\left(\{e_n\}_{n\in\mathbb{N}}, \mathcal{A} \cap [n_0]\right)$ with C_{Ex}.

Asymptotic Tightenings of Thm. 3.7

- By Conlon and Gowers Thm.:

Theorem 3.8

Let be $m \in \mathbb{N}$, and $\delta \in (0,1)$. Given a constant $C_{Ex} > 0$. Then, there is a constant C, s.t.:

$$\lim_{N\to\infty} \mathbb{P}\left(A_{N,m,p}\right) = 1, \quad \textit{if } p > \frac{C}{N^{\frac{1}{m-1}}},$$

where $A_{N,m,p}$ denotes the event: "The PAPR problem is not solvable for $\left(\{e_n\}_{n\in\mathbb{N}}, \mathcal{I}\right)$ with

$$C_{Ex} \leq \frac{\sqrt{m}}{\frac{4}{\pi^2}\log\left(\frac{m}{2}\right) + C},$$

where $C >$ is an absolute constant, for every subset $\mathcal{I} \subset [N]_p$ of size $|\mathcal{I}| \geq \delta\,|[N]_p|$."

Notation: For $N \in \mathbb{N}$ and $p \in [0,1]$, $[N]_p$ denotes a random set in which each element of $[N]$ is chosen independently with probability p.

Outline

Walsh functions

Definition 4.1 (Rademacher -, Walsh Functions)

The *Rademacher functions* r_n, $n \in \mathbb{N}$, on $[0,1]$ are defined as the functions:

$$\mathrm{r}_n(\cdot) := \mathsf{sign}[\sin(\pi 2^n(\cdot))],$$

where sign denotes simply the signum function, with $\mathsf{sign}(0) = -1$.
By means of the Rademacher functions, we can define the so called *Walsh Functions* w_n, $n \in \mathbb{N}$, on $[0,1]$ iteratively by:

$$\mathrm{w}_{2^k+m} = \mathrm{r}_k \mathrm{w}_m, \quad k \in \mathbb{N}_0 \text{ and } m \in [2^k],$$

where w_1 is given by $\mathrm{w}_1(t) = 1$, $t \in [0,1]$.

Basic Properties:

- $\{\mathrm{w}_n\}_{n\in\mathbb{N}}$ forms a multiplicative self-inverse group with the identity w_1. Furthermore, each element is self-inverse.
- $\{\mathrm{w}_n\}_{n\in\mathbb{N}}$ is a complete ONS in $L^2([0,1])$.
- For $n \in \mathbb{N} \setminus 1$, $\int_0^1 \mathrm{w}_n(t)\mathrm{d}t = 0$.

Perfect Walsh Sum

- The following object plays an important role for the derivation of solvability of PAPR problem for CDMA systems.

Definition 4.2 (Perfect Walsh Sum (PWS))

Let be $\mathcal{I} \subset \mathbb{N}$ finite. In case that the Walsh sum f indexed by $\mathcal{I}$, i.e. $f = \sum_{k \in \mathcal{I}} \mathrm{w}_k$ can be represented as:

$$f = \mathrm{w}_{l_*} \prod_{n=1}^{m} (1 + \mathrm{w}_{k_n}) = \mathrm{w}_{l_*} (1 + \sum_{n=1}^{2^m - 1} \mathrm{w}_{l_n}) \tag{3}$$

for a $l_* \in \mathbb{N}$, $l_1, \ldots, l_{2^m-1} \in \mathbb{N} \setminus \{1\}$ mutually distinct, and $k_n \in \mathbb{N}$, for $n \in [m]$, we say f is a perfect Walsh sum (PWS) of size 2^m.

- With abuse of terminology, $\mathcal{I}$ in above Def. is also called PWS of size 2^m.

- The adjective perfect is due to the following elementary property:

Lemma 4.3

Let $m \in \mathbb{N}$. For an perfect Walsh sum f of the size 2^m, it holds:

$$\|f\|_{L^1([0,1])} = 1 \quad \textit{and} \quad \|f\|_{L^2([0,1])} = 2^{\frac{m}{2}}$$

- As an immediate consequence of previous Lemma and the Theorem on the necessary condition for the solvability of PAPR reduction problem, we have:

Lemma 4.4

Let be $\mathcal{I} \subset \mathbb{N}$. Assume that $\mathcal{I}$ contains a PWS of size 2^m. If the PAPR reduction problem is solvable for $(\{\mathrm{w}_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with a given extension constant $C_{\mathsf{Ex}} > 0$, then it follows:

$$C_{\mathsf{Ex}} \geq 2^{\frac{m}{2}}.$$

- Thus, for a $C_{\mathsf{Ex}} > 0$, to show that the PAPR reduction problem is not solvable for $(\{\mathrm{w}_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with C_{Ex}, one needs to check whether a PWS of size 2^m exists in the information set, with $2^{\frac{m}{2}} > C_{\mathsf{Ex}}$.

Existence of PWS in an Information Set

Theorem 4.5

Let be $N = 2^n$, $n \in \mathbb{N}$, and $\delta \in (0,1)$. Then, for every subset $\mathcal{I} \subset [N]$ fulfilling:

$$|\mathcal{I}| \geq \delta N \quad \text{and} \quad |\mathcal{I}| \geq 3\left(\frac{2}{\delta}\right)^{2^m - 1},$$

for an $m \in \mathbb{N}$, $\mathcal{I}$ contains a PWS of size 2^m.

Proof of Thm. 4.5 (Idea)

▷ The following quantity and sets play an important rule for the proof:

Definition 4.6

Let be $\mathcal{I} \subset \mathbb{N}$ finite, and $r \in \mathbb{N}$. The *correlation between* w_r *and* $\mathcal{I}$ is defined as the quantity:

$$\mathsf{Corr}(\mathrm{w}_r, \mathcal{I}) = \int_0^1 \mathrm{w}_r(t) \left| \sum_{k \in \mathcal{I}} \mathrm{w}_k(t) \right|^2 \mathrm{d}t.$$

Furthermore, for w_r, $r \neq 1$, and $\mathcal{I}$, we define the following sets:

- $\mathcal{M}(\mathrm{w}_r, \mathcal{I}) := \left\{ k \in \mathcal{I} : \ \mathrm{w}_k \mathrm{w}_{\tilde{k}} = \mathrm{w}_r, \ \text{for a } \tilde{k} \in \mathcal{I} \right\}$
- $\underline{\mathcal{M}}(\mathrm{w}_r, \mathcal{I}) := \left\{ k \in \mathcal{I} : \ \mathrm{w}_k \mathrm{w}_{\tilde{k}} = \mathrm{w}_r, \ \text{for a } \tilde{k} \in \mathcal{I}, \ \text{with } \tilde{k} > k \right\}$
- $\overline{\mathcal{M}}(\mathrm{w}_r, \mathcal{I}) := \mathcal{M}(\mathrm{w}_r, \mathcal{I}) \setminus \underline{\mathcal{M}}(\mathrm{w}_r, \mathcal{I})$

Proof of Thm. 4.5 (Idea)

- Straightforward to show the following relation between the correlation and subsets defined previously by means of the basic properties of Walsh functions:

Lemma 4.7

Let be $N = 2^n$, $n \in \mathbb{N}$, $\mathcal{I} \subset [N]$, *and* $r \in [N]$. *The following holds:*

1. $|\mathcal{M}(\mathrm{w}_r, \mathcal{I})| = 2\,|\underline{\mathcal{M}}(\mathrm{w}_r, \mathcal{I})| = 2\,\left|\overline{\mathcal{M}}(\mathrm{w}_r, \mathcal{I})\right|$
2. $\mathit{Corr}(\mathrm{w}_r, \mathcal{I}) = |\mathcal{M}(\mathrm{w}_r, \mathcal{I})|$
3. $\sum_{r=1}^{N} \mathit{Corr}(\mathrm{w}_r, \mathcal{I}) = |\mathcal{I}|^2$
4. $\arg\max_{r \in [N]\setminus\{1\}} \mathit{Corr}(\mathrm{w}_r, \mathcal{I}) \geq (|\mathcal{I}|^2 - |\mathcal{I}|)/N$

Proof of Thm. 4.5 (Idea)

- Take a suitable $\delta \in (0,1)$, and let for now $N := 2^n$, $n \in \mathbb{N}$ be arbitrary. Further, take an arbitrary $\mathcal{I} \subset [N]$, which satisfies $|\mathcal{I}| \geq \delta N$.
- **1. step**:
  - Compute $r_1 := \arg\max_{r\in[N]\setminus\{1\}} \mathsf{Corr}(\mathrm{w}_r, \mathcal{I})$, and define $\mathcal{I}_1 := \underline{\mathcal{M}}(\mathrm{w}_{r_1}, \mathcal{I})$.
  - By Lemma 4.7, we can relate $\mathcal{I}_1$ to $\mathsf{Corr}(\mathrm{w}_{r_1}, \mathcal{I})$, and subsequently to $|\mathcal{I}|$ and N:

$$|\mathcal{I}_1| = \frac{1}{2}\,|\mathcal{M}(\mathrm{w}_{r_1}, \mathcal{I})| = \frac{1}{2}\,\mathsf{Corr}(\mathrm{w}_{r_1}, \mathcal{I}) \geq \frac{|\mathcal{I}|\,(|\mathcal{I}|-1)}{2N}$$

  - By assumption, we continue:

$$|\mathcal{I}_1| \geq \frac{\delta}{2}(|\mathcal{I}|-1) > \frac{\delta}{2}(|\mathcal{I}|-2), \tag{4}$$

  - If $\mathcal{I}_1$ is non-empty (By (4), $|\mathcal{I}| \geq 3(2/\delta)$ sufficient), we can write:

$$\sum_{k\in\mathcal{M}(\mathrm{w}_{r_1},\mathcal{I})} \mathrm{w}_k = \sum_{k\in\overline{\mathcal{M}}(\mathrm{w}_{r_1},\mathcal{I})} \mathrm{w}_k + \sum_{\underline{k}\in\underline{\mathcal{M}}(\mathrm{w}_{r_1},\mathcal{I})} \mathrm{w}_{\underline{k}} = (1+\mathrm{w}_{r_1}) \sum_{\underline{k}\in\mathcal{I}_1} \mathrm{w}_{\underline{k}}. \tag{5}$$

$\Rightarrow$ $\forall k \in \mathcal{I}$, $f_k^{(1)} := (1+\mathrm{w}_{r_1})\mathrm{w}_k$ is a Walsh sum indexed by a subset of $\mathcal{M}(\mathrm{w}_{r_1}, \mathcal{I})$.

$\Rightarrow$ $\mathcal{I} \supset \mathcal{M}(\mathrm{w}_{r_1}, \mathcal{I})$ contains a PWS of size 2.

Proof of Thm. 4.5 (Idea)

▷ 2. step:

- Assume that $|\mathcal{I}_1| > (\delta/2)(|\mathcal{I}| - 2)$.
- Compute $r_2 := \arg\max_{r\in[N]\setminus\{1\}} \mathrm{Corr}(\mathrm{w}_r, \mathcal{I}_1)$ (Possible to show: $r_2 \neq r_1$), and define $\mathcal{I}_2 := \underline{\mathcal{M}}(\mathrm{w}_{r_2}, \mathcal{I}_1)$.
- By similar argument as in the 1. step, assumption on $|\mathcal{I}_1|$, and some computations:

$$|\mathcal{I}_2| > \left(\tfrac{\delta}{2}\right)^3 |\mathcal{I}| - 2. \tag{6}$$

- If $\mathcal{I}_2 \neq \emptyset$ (By (6), $|\mathcal{I}| \geq 3(2/\delta)^3$ sufficient), we have

$$\sum_{r\in\mathcal{M}(\mathrm{w}_{r_2},\mathcal{I}_1)} \mathrm{w}_r = (1+\mathrm{w}_{r_2}) \sum_{\underline{r}\in\underline{\mathcal{M}}(\mathrm{w}_{r_2},\mathcal{I}_1)} \mathrm{w}_{\underline{r}},$$

by similar splitting of the sum as done in the 1. step.
- As a consequence, we can continue to expand (5) as:

$$\sum_{r\in\mathcal{M}(\mathrm{w}_{r_1},\mathcal{I})} \mathrm{w}_r = (1+\mathrm{w}_{r_1})(1+\mathrm{w}_{r_2}) \sum_{k\in\mathcal{I}_2} \mathrm{w}_k + f^{(2)}_{\text{rem}},$$

where $f^{(2)}_{\text{rem}}$ is simply some summands in $\sum_{k\in\mathcal{M}(\mathrm{w}_{r_1},\mathcal{I})} \mathrm{w}_k$.

$\Rightarrow$ $\forall k \in \mathcal{I}$, $f^{(2)}_k := (1+\mathrm{w}_{r_1})(1+\mathrm{w}_{r_2})\mathrm{w}_k$ a Walsh sum indexed by a subset of $\mathcal{M}(\mathrm{w}_{r_1}, \mathcal{I})$.

$\Rightarrow$ $\mathcal{I} \supset \mathcal{M}(\mathrm{w}_{r_1}, \mathcal{I})$ contains a PWS of size 2^2.

▷ The remaining follows by repeating the previous 2 steps and by induction.

PAPR reduction problem for CDMA Case - PWS

Theorem 4.8

Given $\delta \in (0,1)$, and assume that $N := 2^n$, $n \in \mathbb{N}$ fulfills:

$$N \geq \frac{3}{2}\left(\frac{2}{\delta}\right)^{2^m} \quad \textit{for some } m \in \mathbb{N}.$$

If the PAPR problem is solvable for $(\{\mathrm{w}_n\}_{n\in\mathbb{N}}, \mathcal{I})$ with constant C_{Ex}, for a subset $\mathcal{I} \subset [N]$ having the density $|\mathcal{I}|/N \geq \delta$, then it holds:

$$C_{Ex} \geq 2^{\frac{m}{2}}.$$

proof idea:

- $|\mathcal{I}| \geq \delta N \geq 3(2/\delta)^{2^m - 1}$.
- Apply Thm. 4.5.

PWS - Asymptotic result

The following consequence of Thm. 4.5 shall be used to give analogons of Conlon and Gower's -, Green and Tao asymptotic results on arithmetic progressions, for PWS:

Corollary 4.9

Let be $m \in \mathbb{N}$ and $N \in \mathbb{N}$ be sufficiently large, s.t.:

$$\delta_N := 2\left(\frac{3}{2N}\right)^{\frac{1}{2^m}} \in (0,1).$$

Then all subsets $\mathcal{I} \subset [N]$, with $|\mathcal{I}| \geq \delta_N N$, contains a PWS of size 2^m.

Proof:

- by Thm. 4.5, a sufficient condition for $\delta \in (0,1)$, s.t. $\mathcal{I} \subset [N]$, with $|\mathcal{I}| \geq \delta N$, contains a PWS of size 2^m:

$$\delta N \geq 3\left(\frac{2}{\delta}\right)^{2^m-1}. \tag{7}$$

- Equality in (7) is achieved by setting $\delta = \delta_N$

PWS - Asymptotic and Probabilistic result

Theorem 4.10

Let be $m \in \mathbb{N}$. Then there is a sequence $\{p_N\}$, with N large enough, in $(0, 1]$ tending to zero, for which it holds:

$$\lim_{N\to\infty} \mathbb{P}\left[[N]_{p_N} \textit{ contains a PWS of size } 2^m\right] = 1$$

Sketch of Proof:

- For $m \in \mathbb{N}$, and $\tau > 1$, choose $N \in \mathbb{N}$ large enough, s.t. $p_N := \tau\delta_N$, where δ_N is given as in Cor. 4.9.
- Since $|[N]_{p_N}|$ is binomially distributed, Chernoff's bound asserts that the probability of $|[N]_{p_N}|$ is getting more concentrated near $\mathbb{E}[|[N]_{p_N}|] = \tau\delta_N N$ as N gets larger.
- Cor. 4.9 gives the remaining.

PWS - Asymptotic and Probabilistic result

By some efforts, one can even show a stronger statement:

Theorem 4.11

Let $m \in \mathbb{N}$, and $\delta \in (0,1)$. Then there is a sequence $\{p_N\}$, with N large enough, in $(0,1]$, tending to zero, for which it holds:

$$\lim_{N \to \infty} \mathbb{P}\left[A_{N,m,\delta}\right] = 1,$$

where $A_{N,m,\delta}$ denotes the event:
"Every subset $\mathcal{I}$ of $[N]_{p_N}$, with $|\mathcal{I}| \geq \delta \left|[N]_{p_N}\right|$ contains a PWS of size 2^m."

PWS & Solvability of PAPR Reduction Problem - Asymptotic and Probabilistic result

Theorem 4.12

Let be $m \in \mathbb{N}$*. Given an extension constant* $C_{Ex} > 0$*, with* $C_{Ex} < 2^{\frac{m}{2}}$*. Then there exists a sequence* $\{p_N\}$*, with* N *large enough, in* $(0, 1]$*, tending to zero, s.t.:*

$$\lim_{N\to\infty} \mathbb{P}\left[\textit{The PAPR problem is not solvable for } (\{\mathrm{w}_n\}_{n\in\mathbb{N}}, [N]_{p_N}) \textit{ with } C_{Ex}\right] = 1$$

PWS & Solvability of PAPR Reduction Problem - Asymptotic and Probabilistic result

Theorem 4.13

Let be $m \in \mathbb{N}$. Given an extension constant $C_{\mathsf{Ex}} > 0$, with $C_{\mathsf{Ex}} < 2^{\frac{m}{2}}$, and $\delta > 0$. Then there exists a sequence $\{p_N\}$, with N large enough, in $(0, 1]$, tending to 0, for which it holds:

$$\lim_{N \to \infty} \mathbb{P}\left[B_{N,\delta}\right] = 1,$$

where $B_{N,\delta}$ denotes the event:
"The PAPR problem is not solvable for all $(\{\mathrm{w}_n\}_{n \in \mathbb{N}}, \mathcal{I})$ with C_{Ex}, where $\mathcal{I} \subset [N]_{p_N}$, $|\mathcal{I}| \geq \delta \left|[N]_{p_N}\right|$."

Asymptotic results for PWS

▷ Erdös Conjecture on arithmetic progressions:

If $\mathcal{A} \subset \mathbb{N}$ fulfills $\sum_{k \in \mathcal{A}} 1/k = \infty$, then $\mathcal{A}$ contains arithmetic progressions of arbitrary length.

↯ Still widely open. Even unknown for arithmetic progressions of length 3

▷ By means of Cor. 4.9, we are able to give the solution of Erdös problem for PWS:

Theorem 4.14 (Solution of Erdös Problem for PWS)

Let be $\mathcal{I} \subset \mathbb{N}$, for which it holds: $\sum\limits_{k \in \mathcal{I}} \frac{1}{k} = \infty$. Then, $\mathcal{I}$ contains a PWS of arbitrary size. Specifically: For each $m \in \mathbb{N}$, there exists $n_0 \in \mathbb{N}$, such that $\mathcal{I} \cap [2^{n_0}]$ contains a PWS of size m.

Asymptotic results for PWS

- As an immediate consequence, we obtain the analogon of Green and Tao's Thm. on the existence of arithmetic progressions for PWS:

Corollary 4.15

Let $\mathcal{P} \subset \mathbb{N}$ denotes the set of prime numbers. Then, $\mathcal{P}$ contains an PWS of arbitrary length, i.e. for every $m \in \mathbb{N}$, there exists $n_0 \in \mathbb{N}$, s.t. $\mathcal{P} \cap [2^{n_0}]$ contains a PWS of size 2^m.

Asymptotic results for PWS

- As an immediate consequence, we obtain the analogon of Green and Tao's Thm. on the existence of arithmetic progressions for PWS:

Corollary 4.16

Let $\mathcal{P} \subset \mathbb{N}$ denotes the set of prime numbers. Then, $\mathcal{P}$ contains an PWS of arbitrary length, i.e. for every $m \in \mathbb{N}$, there exists $n_0 \in \mathbb{N}$, s.t. $\mathcal{P} \cap [2^{n_0}]$ contains a PWS of size 2^m.

- Immediate consequence for the Solvability of PAPR Problem for CDMA:

For an information set $\mathcal{I} \subset \mathbb{N}$, with $\sum_{k \in \mathcal{I}} 1/k = \infty$, the PAPR reduction is not solvable for $(\{\mathrm{w}_n\}_{n \in \mathbb{N}}, \mathcal{I})$ with any extension constant $C_{Ex} > 0$.

Outline

Summary and Conclusions

- ▷ High dynamics of orthogonal transmission scheme is a serious problem.
- ▷ Tone reservation gives a canonical method to control the peak value of waveforms of orthogonal transmission scheme.
  - ↯ Not applicable for arbitrary cases, specifically: for any desired threshold value!
- ▷ PAPR reduction problem is related to several interesting mathematical fields, such as functional analysis, (additive) combinatorics, trigonometric -, and non-trigonometric analysis.
- ▷ The solvability of PAPR reduction problem for an orthogonal transmission scheme with a given extension constant (resp. the applicability of tone reservation method for a given threshold value) depends on the existence of certain combinatorial objects:
  - In the OFDM/Fourier case: Arithmetic progressions
    - ⇒ The famous Szemerédi Thm. and several tightening due to Green and Tao, Conlon and Gowers can be applied.
    - ↯ The deterministic asymptotic case still open (Erdös Conjencture).
  - In the CDMA/Walsh case: Perfect Walsh sum
    - ⇒ Szémeredi-like Theorem and several tightening for the asymptotic case can be derived.
    - ⇒ A solution to the Erdös problem can even be given in this case.

„Das Buch der Natur ist in der Sprache der Mathematik geschrieben [...], ohne die es ganz unmöglich ist auch nur einen Satz zu verstehen, ohne die man sich in einem dunklen Labyrinth verliert.“

— Galileo Galilei, Il Saggiatore (1623)

Thank You!

▷ Questions?

Remarks?