Graduate J. Math. 1 (2016), 59 – 78

Subgaussian sequences in probability and Fourier analysis

Gilles Pisier

Abstract

This is a review on subgaussian sequences of random variables, prepared for the Mediterranean Institute for the Mathematical Sciences (MIMS). We first describe the main examples of such sequences. Then we focus on examples coming from the harmonic analysis of Fourier series and we describe the connection of subgaussian sequences of characters on the unidimensional torus (or any compact Abelian group) with Sidon sets. We explain the main combinatorial open problem concerning such subgaussian sequences. We present the answer to the analogous question for subgaussian bounded mean oscillation (BMO) sequences on the unit circle. Lastly, we describe several very recent results that provide a generalization of the preceding ones when the trigonometric system (or its analogue on a compact Abelian group) is replaced by an arbitrary orthonormal system bounded in L_∞.

MSC 2010. Primary: 60G15, 43A46; Secondary: 42A16, 42A55.

A sequence (f_n) of real valued random variables is called subgaussian if there is $s \geq 0$ such that for any finitely supported $(x_n) \in \mathbb{R}^{\mathbb{N}}$

$$\mathbb{E} \exp\left(\sum x_n f_n\right) \leq \exp(s^2 \sum x_n^2/2). \qquad (0.1)$$

The equality case corresponds to Gaussian independent variables with the same variance. A similar definition (see below) can be given for the $\mathbb{C}$-valued case. Then the family is subgaussian if and only if (iff in short) the family that is the union of the real and imaginary parts of (f_n) is subgaussian in the real sense.

As we will show, this notion plays an important role in Gaussian process theory and in the harmonic analysis of thin sets, such as Sidon sets. In fact, as will be shown in §9, a subsequence of the trigonometric system of the form $f_n(t) = \exp(ik(n)t)$ (with $k(n)$ distinct integers in $\mathbb{Z}$) is subgaussian on $([0, 2\pi], dt/2\pi)$ iff it is a Sidon sequence, i.e. one for which any continuous function φ on the unit circle (identified as usual with $\mathbb{R}/2\pi\mathbb{Z}$) with Fourier transform $\widehat{\varphi}$ supported by the set $\{k(n)\}$ has an absolutely convergent Fourier series

$$\varphi(t) = \sum \widehat{\varphi}(k(n)) \exp(ik(n)t).$$

It turns out that much of the connection between subgaussian and Sidon sequences remains valid for general uniformly bounded orthonormal systems. This came as a surprise since it was generally believed that the group structure played a key role. This very recent development from [5, 27] is described in §10.

The important feature of subgaussian sequences is that although they share many properties of bounded independent random variables, they actually seem much more general. The notion of subgaussian seems somewhat transversal in probability theory : it interacts with many fundamental topics such as Gaussian processes, martingales, Orlicz spaces, Fourier series or isoperimetric inequalities (see e.g. [24, 30, 17, 19, 22, 32]) but it can never be reduced to the intersection with any of these topics. As we will explain in §7, there is a major open problem that proposes a characterization of subgaussian sequences in the Fourier series framework. The true meaning of subgaussian remains puzzling. The more recent results on uniformly bounded orthonormal systems described at the end of the paper give some hope to make progress to clarify that.

1 Gaussian and subgaussian variables

In this paper, a real valued Gaussian random variable g on a probability space $(\Omega, \mathbb{P})$ is called Gaussian if there is $\sigma \geq 0$ such that for any measurable $A \subset \mathbb{R}$

$$\mathbb{P}\{g \in A\} = \int_A e^{-x^2/2\sigma^2} dx/\sqrt{2\pi}\sigma.$$

Note that *we only consider Gaussian variables with mean* 0.
Then σ^2 is the variance of g and $\mathbb{E}g^2 = \sigma^2$. When $\sigma = 1$, g is called normal. We have then

$$\forall z \in \mathbb{C} \quad \mathbb{E} \exp(zg) = \exp z^2/2.$$

A complex valued random variable g is called $\mathbb{C}$-Gaussian (resp. $\mathbb{C}$-Gaussian normal) if its real and imaginary parts are independent Gaussian with the same variance σ (resp. with variance 1). We have then when $\sigma = 1$

$$\forall z \in \mathbb{C} \quad \mathbb{E}\exp(\Re(zg)) = \mathbb{E}\exp(\Re(\bar{z}g)) = \exp|z|^2/2.$$

Warning: with this convention, a nonzero real valued Gaussian variable is not $\mathbb{C}$-Gaussian !

We also need a variant: a $\mathbb{C}$-Gaussian variable will be called normalized if $\mathbb{E}|g|^2 = 1$ (note that for a normal $\mathbb{C}$-Gaussian variable we have $\mathbb{E}|g|^2 = 2$).

For convenience, we will sometimes call $\mathbb{R}$-Gaussian any real valued Gaussian random variable. We will say that it is normalized if its L_2-norm is 1. In the real case this is the same as normal.

Let (g_n) be an i.i.d. sequence of normalized $\mathbb{R}$-Gaussian (resp. $\mathbb{C}$-Gaussian) variables. Note that this is an orthonormal system in $L_2(\Omega, \mathbb{P})$. Then for any (nonzero) sequence $x = (x_n) \in \ell_2$, the variable $g = (\sum |x_n|^2)^{-1/2} \sum x_n g_n$ is a standard Gaussian variable. Therefore

$$\| \sum x_n g_n \|_p = \|g_1\|_p (\sum |x_n|^2)^{1/2}. \tag{1.1}$$

In the real case (with $x_n \in \mathbb{R}\ \forall n$)

$$\mathbb{E}\exp(\sum x_n g_n) = \exp(\sum x_n^2/2). \tag{1.2}$$

In the complex case, assuming (g_n) $\mathbb{C}$-Gaussian normal (with $x_n \in \mathbb{C}\ \forall n$)

$$\mathbb{E}\exp(\Re(\sum x_n g_n)) = \exp(\sum |x_n|^2/2). \tag{1.3}$$

Definition. A real valued random variable f is called subgaussian if there is a constant $s \geq 0$ such that for any $x \in \mathbb{R}$

$$\mathbb{E}\exp xf \leq \exp s^2x^2/2. \tag{1.4}$$

As is well known this implies that for any $c > 0$

$$\mathbb{P}(\{f > c\}) \leq \exp -(c^2/2s^2) \tag{1.5}$$

and also

$$\mathbb{P}(\{f < -c\}) \leq \exp -(c^2/2s^2). \tag{1.6}$$

Indeed, by Markov's inequality we have for any $x > 0$ $\mathbb{P}(\{f > c\}) \leq \exp(s^2x^2/2 - xc)$ and the choice of $x = c/s^2$ yields (1.5). Then (1.6) follows by applying (1.5) to $-f$.

A complex valued random variable f is called $\mathbb{C}$-subgaussian if there is constant $s \geq 0$ such that for any $x \in \mathbb{C}$

$$\mathbb{E}\exp \Re(xf) \leq \exp s^2|x|^2/2. \tag{1.7}$$

A real valued sequence (f_n) is called subgaussian if there is $s \geq 0$ such that for any $(x_n) \in \mathbb{R}^{\mathbb{N}}$ in the unit sphere of ℓ_2 the variable $f = \sum x_n f_n$ satisfies (1.4). Equivalently, for any finitely supported $(x_n) \in \mathbb{R}^{\mathbb{N}}$

$$\mathbb{E}\exp(\sum x_n f_n) \leq \exp(s^2 \sum x_n^2/2). \tag{1.8}$$

A complex valued sequence (f_n) is called $\mathbb{C}$-subgaussian if the real valued sequence formed together by both its real parts $(\Re f_n)$ and its imaginary parts $(\Im f_n)$ is subgaussian in the preceding sense. This implies that for some $s \geq 0$ for any finitely supported $(x_n) \in \mathbb{C}^{\mathbb{N}}$

$$\mathbb{E}\exp(\Re(\sum x_n f_n)) \leq \exp(s^2 \sum |x_n|^2/2). \tag{1.9}$$

Moreover, we denote by $sg(f)$ (resp. $sg(\{f_n\})$) the smallest number $s \geq 0$ for which this holds.

The following are immediate consequences of the definition:

Lemma 1.1. *If f is $\mathbb{R}$-subgaussian (resp. $\mathbb{C}$-subgaussian) then so is tf for any $t \in \mathbb{R}$ (resp. $t \in \mathbb{C}$) and $sg(tf) = |t| sg(f)$. Also $\mathbb{E}(f) = 0$ and in the real case $\mathbb{E}f^2 \leq sg(f)^2$.*
Let f_1, f_2 be two subgaussian variables (either both real or both complex). Then

$$sg(f_1 + f_2) \leq \sqrt{2}(sg(f_1)^2 + sg(f_2)^2)^{1/2}. \tag{1.10}$$

Moreover, if (f_n) is an independent sequence of $\mathbb{R}$-subgaussian (resp. $\mathbb{C}$-subgaussian) variables such that $\sum sg(\{f_n\})^2 < \infty$, then $f = \sum f_n$ is $\mathbb{R}$-subgaussian (resp. $\mathbb{C}$-subgaussian) with $sg(f) \leq (\sum sg(\{f_n\})^2)^{1/2}$.

Proof. (1.10) follows from the easy (and soft) observation that if in the real valued case $s_1 = sg(f_1)$ and $s_2 = sg(f_2)$, we have by Cauchy-Schwarz for any $x \in \mathbb{R}$

$$\begin{aligned} &\int \exp(x(f_1 + f_2))dm \\ &\leq \left(\int \exp(2xf_1)dm \int \exp(2xf_2)dm \right)^{1/2} \\ &\leq \left(\exp(2x^2s_1^2)\exp(2x^2s_2^2) \right)^{1/2} \\ &= \exp(x^2(s_1^2 + s_2^2)). \end{aligned}$$

The other assertions are left to the reader. □

Concerning (1.10), we will show later (see Lemma 3.2) that $f \mapsto sg(f)$ is equivalent to a norm, namely $f \mapsto \|f\|_{\psi_2}$.

In the real valued case we sometimes use the term $\mathbb{R}$-subgaussian instead of subgaussian.

Of course, $\mathbb{R}$-Gaussian (resp. $\mathbb{C}$-Gaussian) implies $\mathbb{R}$-subgaussian (resp. $\mathbb{C}$-subgaussian), and for a normal Gaussian variable g we have $sg(g) = 1$.

A simple and basic non-Gaussian example is given by a sequence (ε_n) of independent choices of signs $\varepsilon_n = \pm 1$ taking the values ± 1 with equal probability 1/2. Then one has $sg(\{\varepsilon_n\}) = 1$. This follows simply from

$$\forall x \in \mathbb{R} \quad \cosh(x) \leq \exp(x^2/2), \tag{1.11}$$

which just follows from Stirling's formula:

$$\cosh(x) = 1 + \sum_1^\infty x^{2n}/(2n)! \leq 1 + \sum_1^\infty x^{2n}/(2^n n!).$$

More generally, by an inequality due to Azuma [2], martingale increments satisfy the same:

Theorem 1.2. *Let $(f_n)_{n\geq 0}$ be a real valued martingale in L_1 on some probability space. Let $d_n = f_n - f_{n-1}$ $(n \geq 1)$. Then if $\|d_n\|_\infty \leq 1$ for any $n \geq 1$, the sequence (d_n) is subgaussian with $sg(\{d_n\}) \leq 1$.*

Proof. We will use the following elementary bound: for any $t \in \mathbb{R}$

$$\forall d \in [-1, 1] \quad , \quad \exp(xd) \leq \cosh(x) + d \sinh(x). \quad (1.12)$$

Indeed, by the convexity of $d \to \exp(xd)$ on $[-1, 1]$, since $d = 2^{-1}(d+1)(1) + 2^{-1}(1-d)(-1)$ we have

$$\exp(xd) \leq 2^{-1}(d+1)\exp(x) + 2^{-1}(1-d)\exp(-x),$$

which proves this bound.

Let $M_n = \sum_1^n x_k d_k$. Clearly (M_n) is a martingale relative to the filtration associated to (f_n). We denote by $\mathbb{E}_n$ the conditional expectation with respect to $\sigma\{M_k \mid k \leq n\}$ and we set $M_0 = 0$. We now claim that for any $n \geq 1$

$$\mathbb{E}_{n-1} \exp(M_n) \leq \exp(M_{n-1}) \exp\left(x_n^2/2\right).$$

Note $M_n - M_{n-1} = t_n d_n$. We have by (1.12) and by (1.11)

$$\begin{aligned}
&\mathbb{E}_{n-1} \exp M_n \\
&\quad \leq \exp(M_{n-1}) \mathbb{E}_{n-1}[\cosh(x_n) + d_n \sinh(x_n)] \\
&\quad = \exp(M_{n-1}) \cosh(x_n) \\
&\quad \leq \exp(M_{n-1}) \exp(x_n^2/2)
\end{aligned}$$

which proves the claim. Now

$$\begin{aligned}
\mathbb{E}\exp(M_n) &= \mathbb{E}\mathbb{E}_{n-1} \exp M_n \\
&\leq \mathbb{E}\exp(M_{n-1}) \exp(x_n^2/2),
\end{aligned}$$

and hence by induction

$$\mathbb{E}\exp(M_n) \leq \exp\left(\sum_1^n x_k^2/2\right).$$

□

Remark 1.3. The most basic example of subgaussian sequence is a sequence (ε_n) of independent choices of signs, i.e. an i.i.d. sequence of ± 1-valued variables with $\mathbb{P}(\{\varepsilon_n = \pm 1\}) = 1/2$. This classical example is of course included in those given by the preceding statement since the partial sums $S_n = \sum_1^n \varepsilon_k$ form a martingale. Note that

$$sg(\{\varepsilon_n\}) = 1 \quad \text{and} \quad sg(\sum\nolimits_1^n \varepsilon_k) \leq \sqrt{n}. \quad (1.13)$$

The complex analogue of (ε_n) is a sequence (z_n) of i.i.d. random variables with values in the unit circle $\mathbb{T}$ of $\mathbb{C}$ with distribution equal to the normalized Haar measure on $\mathbb{T}$. This sequence is $\mathbb{C}$-subgaussian with $sg(\{z_n\}) \leq 1$. Indeed, for any finitely supported $(x_n) \in \mathbb{C}^{\mathbb{N}}$, the variables (d_n) defined by $d_n = \Re(x_n z_n)|x_n|^{-1}$ (with the convention $0/0 = 0$), being independent with mean 0 form a sequence of martingale differences with $|d_n| \leq 1$. Thus by Theorem 1.2 $sg(\{d_n\}) \leq 1$, which implies $sg(|x_n| d_n) \leq |x_n|$. Now by Lemma 1.1, if $\sum |x_n|^2 = 1$ then $sg(\sum x_n z_n) \leq 1$. Thus we conclude that

$$sg(\{z_n\}) \leq 1.$$

Another important example of subgaussian random variable can be derived from the fundamental isoperimetric inequality for Gaussian measure and the related concentration phenomenon:

Theorem 1.4. *Let $F : \mathbb{R}^n \to \mathbb{R}^n$ be a mapping (a priori non-linear) satisfying the Lipschitz condition:*

$$\forall x, y \in \mathbb{R}^n \quad \|F(x) - F(y)\|_2 \leq \|x - y\|_2. \quad (1.14)$$

Let $(g_1, \cdots, g_n)$ be i.i.d. normal $\mathbb{R}$-Gaussian variables. Then the variables

$$f_j = F_j(g_1, \cdots, g_n) - \mathbb{E}F_j(g_1, \cdots, g_n)$$

are subgaussian with $sg(\{f_j\}) \leq 1$.

We will give two proofs. First following [30, p. 181] we review a proof due to Maurey using Brownian stochastic integrals and Azuma's inequality (1.2). A similar proof already appears in [7, p. 26] (but we were not aware of that reference at the time [30, p. 181] was written). See also [7, 36], for closely related results. See also the exposition in [1, chap. 3], for the connection with isoperimetric inequalities.

Let us sketch Maurey's argument. Fix $x \in \mathbb{R}^n$ with $\|x\|_2 = 1$. It suffices to show that the variable

$$\Phi = \sum\nolimits_{j=1}^n x_j F_j(g_1, \cdots, g_n)$$

is subgaussian with $sg(\Phi) \leq 1$. This rests on the formula

$$\Phi(B_1) - \mathbb{E}\Phi(B_1) = \int_0^1 \nabla(P_{1-t}\Phi)(B_t).dB_t, \quad (1.15)$$

where (B_t) is the standard Brownian motion starting at 0 on $\mathbb{R}^n$, and P_t is the associated Markov semigroup. By Lebesgue's classical differentiation results, we know that (1.14) implies $\|\nabla(\Phi)\|_2 \leq 1$ a.s., but since $P_{1-t}F$ still satisfies (1.14), we also have $\|\nabla(P_{1-t}\Phi)\|_2 \leq 1$ a.s. and we can rewrite (1.15) as

$$\Phi(B_1) - \mathbb{E}\Phi(B_1) = \int_0^1 V_t.dB_t \quad (1.16)$$

with (V_t) such that $\|V_t\|_2 \leq 1$ a.s. for all $0 < t < 1$. Fix $x \in \mathbb{R}$. Now easy arguments from stochastic integration tell us that the process

$$M_s = \exp{(x \int_0^s V_t.dB_t - x^2 s/2)}$$

$(0 \le s \le 1)$ is a supermartingale and hence

$$\mathbb{E}M_1 \le \mathbb{E}M_0 = 1.$$

This last inequality means that $sg(\Phi) \le 1$, which proves Theorem 1.4.

The second proof (also from [30]) is very simple and more elementary but it only shows that

$$sg(\{f_j\}) \le (\pi/2)^2.$$

It runs as follows. Let $g' = (g'_1, \cdots, g'_n)$ be an independent copy of $g = (g_1, \cdots, g_n)$. Then, let

$$g(t) = g\sin(t) + g'\cos(t).$$

Note $g(\pi/2) = g$ and $g(0) = g'$. Let $g'(t) = \frac{d}{dt}g(t) = g\cos(t) - g'\sin(t)$. The key observation is that for any t the pair (g, g') has the same distribution as $(g(t), g'(t))$ (indeed these are Gaussian random vectors in $\mathbb{R}^{2n}$ with the same covariance). Then the proof boils down to "the fundamental formula of calculus", namely

$$\begin{aligned}\Phi(g) - \Phi(g') &= \Phi(g(\pi/2)) - \Phi(g(0))\\ &= \int_0^{\pi/2} \frac{d}{dt}\Phi(g(t))dt\\ &= \int_0^{\pi/2} \nabla\Phi(g(t)).g'(t)dt.\end{aligned}$$

Then by the convexity of the exponential function

$$\begin{aligned}&\mathbb{E}\exp(\Phi(g) - \Phi(g'))\\ &\le \frac{2}{\pi}\int_0^{\pi/2}\left(\mathbb{E}\exp(\frac{\pi}{2}\nabla\Phi(g(t)).g'(t))\right)dt, \quad (1.17)\end{aligned}$$

but by the distributional invariance of $(g(t), g'(t))$, we have by (1.2)

$$\begin{aligned}\forall t \quad &\mathbb{E}\exp(\frac{\pi}{2}\nabla\Phi(g(t)).g'(t)) = \mathbb{E}\exp(\frac{\pi}{2}\nabla\Phi(g).g')\\ &= \mathbb{E}\exp((\frac{\pi}{2})^2\|\nabla\Phi(g)\|_2^2/2)\\ &\le \exp((\frac{\pi}{2})^2/2),\end{aligned}$$

and hence by (1.17)

$$\mathbb{E}\exp(\Phi(g) - \Phi(g')) \le \exp((\frac{\pi}{2})^2/2).$$

This means that $sg(\{F_j(g) - F_j(g')\}) \le (\pi/2)^2$. Since, again by convexity of the exponential, we have

$$\mathbb{E}\exp(\Phi(g) - \mathbb{E}\Phi(g)) \le \mathbb{E}\exp(\Phi(g) - \Phi(g')),$$

we obtain a fortiori $sg(\{F_j(g) - \mathbb{E}F_j(g)\}) \le (\pi/2)^2$.

2 The Mehler kernel (Ornstein-Uhlenbeck semigroup)

For further use at the end of this paper, we need to describe some basic facts about the Mehler kernel. Let $\{g_n \mid 1 \le n \le N\}$ be an i.i.d. sequence of normalized $\mathbb{R}$-Gaussian variables on $(\Omega, \mathcal{A}, \mathbb{P})$, where $\mathcal{A}$ is the σ-algebra generated by $\{g_n \mid 1 \le n \le N\}$.
Let (h_n) $(n \ge 0)$ be the Hermite polynomials on $\mathbb{R}$. Recall $h_0 = 1$, $h_1(x) = x$.
For any $\alpha = (n(1), \cdots, n(N)) \in \mathbb{N}^N$, let

$$h_\alpha(x_1, \cdots, x_N) = h_{n(1)}(x_1)\cdots h_{n(N)}(x_N).$$

We call $d = n(1)+\cdots+n(N)$ the degree of h_α. It is well known that the family of Hermite polynomials (suitably normalized) $\{h_\alpha(g_1, \cdots, g_N)\}$ forms an orthonormal basis of $L_2(\mathbb{P})$. Let P_0 be the orthogonal projection onto the constant functions, and let P_1 be the orthogonal projection onto span$[g_n \mid 1 \le n \le N]$. More generally, we denote by P_d the orthogonal projection onto the span of the Hermite polynomials of degree d in $\{g_n \mid 1 \le n \le N\}$. For any $\delta \in [-1, 1]$ the operator $T_\delta : L_2(\mathbb{P}) \to L_2(\mathbb{P})$ defined by

$$T_\delta = \sum\nolimits_0^\infty \delta^d P_d$$

is a positive contraction on $L_p(\mathbb{P})$ for all $1 \le p \le \infty$.

It is well known that for any smooth enough (e.g. polynomial) function $F(g_1, \cdots, g_N)$ in $L_1(\mathbb{P})$ we have

$$(T_\delta F)(g) = \mathbb{E}_{g'}F(\delta g + (1-\delta^2)^{1/2}g')$$

where $g' = (g'_n)$ is an independent copy of $\{g_n \mid 1 \le n \le N\}$. This is sometimes called Mehler's formula. The operators $t \mapsto T_{e^{-t}}$ form the famous Ornstein-Uhlenbeck semigroup.

It is an easy exercise to show that if $-1 < \delta < 1$ the operator T_δ is given by a positive kernel $K_\delta \in L_1(\mathbb{P}\times\mathbb{P})$, in the sense that for any polynomials F_1, F_2 we have

$$\langle T_\delta(F_1), F_2\rangle = \mathbb{E}_g\mathbb{E}_{g'}K_\delta(g, g')F_1(g')F_2(g).$$

Note that

$$\|K_\delta\|_{L_1(\mathbb{P}\times\mathbb{P})} = \langle T_\delta(1), 1\rangle = 1.$$

The explicit value of K_δ can be easily derived from Mehler's formula. Indeed, assuming for simplicity that $\Omega = \mathbb{R}^N$ equipped with

$$\mathbb{P} = \exp -(\sum x_j^2/2)dx_1\cdots dx_N(2\pi)^{-N/2}$$

and that $\{g_n \mid 1 \le n \le N\}$ are the coordinates on $\mathbb{R}^N$, we have

$$\begin{aligned}&(T_\delta F)(x) = \int F(\delta x + (1-\delta^2)^{1/2}y)\mathbb{P}(dy)\\ &= (2\pi(1-\delta^2))^{-\frac{N}{2}}\int F(t)\exp -(\frac{|t-\delta x|_2^2}{2(1-\delta^2)})dt_1\cdots dt_N\end{aligned}$$

from which we derive

$$K(x,t) = (1-\delta^2)^{-N/2}\exp -(\frac{|t-\delta x|_2^2}{2(1-\delta^2)})\exp(|t|_2^2/2)$$

and finally

$$K(x,t) = (1-\delta^2)^{-N/2} \exp \frac{-\delta^2|t|_2^2 + 2\delta t.x - \delta^2|x|_2^2}{2(1-\delta^2)}.$$

We will invoke the following simple fact.

Lemma 2.1. *For any $z = (z_n) \in [-1,1]^N$ there is a positive operator $\Theta_z : L_1(\mathbb{P}) \to L_1(\mathbb{P})$ of norm 1 such that*

$$\forall n = 1, \cdots, N \quad \Theta_z(g_n) = z_n g_n.$$

Proof. Let $T_\delta^{(1)}$ be the operator corresponding to T_δ in the case $N = 1$. Then we simply may take

$$\Theta_z = T_{z_1}^{(1)} \otimes \cdots \otimes T_{z_N}^{(1)}.$$

□

3 Orlicz spaces of subgaussian variables

We now turn to the behaviour of subgaussian variables in L_p for $p < \infty$. We start by recalling the definition of certain Orlicz spaces. The latter are analogues of the L_p-spaces obtained when one replaces the function $x \mapsto x^p$ by a more general convex increasing function $\psi : \mathbb{R}+ \to \mathbb{R}+$ such that $\psi(0) = 0$.
Let (Ω, m) be a measure space. The Orlicz space $L_\psi(\Omega, m)$ (or $L_\psi(m)$, or simply L_ψ) is the space of those $f \in L_0(\Omega, m)$ for which there is $t > 0$ such that $\mathbb{E}\psi(|f|/t) < \infty$ and we set

$$\|f\|_\psi = \inf\{t > 0 \mid \mathbb{E}\psi(|f|/t) \le \psi(1)\}.$$

It is known that the resulting space is a Banach space and, if m is finite, we have $L_\infty \subset L_\psi \subset L_1$.

We will be interested by the particular case of exponentially growing functions, so we limit our discussion to that special case. Let $0 < a < \infty$. Let

$$\forall x > 0 \quad \psi_a(x) = \exp x^a - 1.$$

Then

$$\|f\|_{\psi_a} = \inf\{t > 0 \mid \mathbb{E}\exp|f/t|^a \le e\}.$$

In many cases the growth of the L_p-norms of a function when $p \to \infty$ is equivalent to its exponential integrability, as in the following elementary and well known Lemma.

Lemma 3.1. *Fix a number $a > 0$. The following properties of a (real or complex) random variable f are equivalent:*

(i) $f \in L_p$ *for all* $p < \infty$ *and* $\sup_{p\ge1} p^{-1/a}\|f\|_p < \infty$.

(ii) $f \in L_{\psi_a}$.

(iii) There is $t > 0$ *such that* $\sup_{c>0} \exp(tc^a)\mathbb{P}\{|f| > c\} < \infty$.

(iv) Let (f_n) *be an i.i.d. sequence of copies of* f. *Then*

$$\sup_n(\log(n+1))^{-1/a}|f_n| < \infty \ a.s. \ .$$

Moreover, there is a positive constant C_a such that for any $f \ge 0$ we have

$$\begin{aligned} C_a^{-1}\sup_{p\ge1} p^{-1/a}\|f\|_p &\le \|f\|_{\psi_a} \qquad (3.1)\\ &\le C_a \sup_{p\ge1} p^{-1/a}\|f\|_p, \end{aligned}$$

and we can restrict the sup over p to be over all even integers.

Proof. Assume that the supremum in (i) is ≤ 1. Then

$$\begin{aligned} \mathbb{E}\exp|f/t|^a &= 1 + \textstyle\sum_1^\infty \mathbb{E}|f/t|^{an}(n!)^{-1}\\ &\le 1 + \textstyle\sum_1^\infty (an)^n t^{-an}(n!)^{-1} \end{aligned}$$

hence by Stirling's formula for some constant C

$$\begin{aligned} \mathbb{E}\exp|f/t|^a &\le 1 + C\textstyle\sum_1^\infty (an)^n t^{-an} n^{-n} e^n\\ &= 1 + C\textstyle\sum_1^\infty (at^{-a}e)^n \end{aligned}$$

from which it becomes clear (since $1 < e$) that (i) implies (ii). Conversely, if (ii) holds we have a fortiori for all $n \ge 1$

$$(n!)^{-1}\|f/t\|_{an}^{an} \le \mathbb{E}\exp|f/t|^a \le e$$

and hence

$$\|f\|_{an} \le e^{\frac{1}{an}}(n!)^{\frac{1}{an}} t \le e^{\frac{1}{a}} n^{\frac{1}{a}} t = (an)^{\frac{1}{a}} t(e/a)^{1/a},$$

which gives $\|f\|_p \le p^{1/a}t(e/a)^{1/a}$ for the values $p = an$, $n = 1, 2, \ldots$. One can then easily interpolate (using Hölder's inequality) to obtain (i). The equivalences of (ii) with (iii) and (iv) are elementary exercises. The last assertion is a simple recapitulation left to the reader.

□

The following variant explains why the variables with $\|f\|_{\psi_2} < \infty$ are sometimes called subgaussian.

Lemma 3.2. *Let $f \in L_1(\Omega, \mathbb{P})$ be real valued such that $\mathbb{E}f = 0$. Then $f \in L_{\psi_2}$ iff f is subgaussian.*
Moreover, $\|f\|_{\psi_2}$, $\sup_{p\ge1} p^{-1/2}\|f\|_p$ and $sg(f)$ are equivalent quantities for such f's.

Proof. Assume that $f \in L_{\psi_2}$ with $\|f\|_{\psi_2} \le 1$. Let f' be an independent copy of f. Let $F = f - f'$. Note that since the distribution of F is symmetric all its odd moments vanish, and hence

$$\mathbb{E}\exp xF = 1 + \textstyle\sum_{n\ge1} \frac{x^{2n}}{2n!}\mathbb{E}F^{2n}.$$

We have $\|F\|_{\psi_2} \le \|f\|_{\psi_2} + \|f'\|_{\psi_2} \le 2$. Therefore $\mathbb{E}(F/2)^{2n} \le n!\mathbb{E}\exp(F/2)^2 \le en!$. Therefore

$$\begin{aligned}\mathbb{E}\exp xF &\le 1 + \sum\nolimits_{n\ge1} \frac{(2x)^{2n}}{2n!} en!\\ &\le 1 + \sum\nolimits_{n\ge1} \frac{(2\sqrt{e}x)^{2n}}{n!}\\ &\le \exp(4ex^2).\end{aligned}$$

But since $t \mapsto \exp -xt$ is convex for any $x \in \mathbb{R}$, and $\mathbb{E}f' = 0$ we have $1 = e^0 \le \mathbb{E}\exp -xf'$ and hence $\mathbb{E}\exp xF = \mathbb{E}\exp xf\mathbb{E}\exp -xf' \ge \mathbb{E}\exp xf$. Thus we conclude $sg(f) \le (8e)^{1/2}$. By homogeneity this shows $sg(f) \le (8e)^{1/2}\|f\|_{\psi_2}$.
Conversely, assume $sg(f) \le 1$. Then by (1.5) and (1.6)

$$\mathbb{P}(\{|f| > t\}) \le 2e^{-t^2/2}.$$

Fix $c > \sqrt{2}$. Let $\theta = 1/2 - 1/c^2$. Note $\theta > 0$. We have

$$\begin{aligned}&\mathbb{E}\exp(f/c)^2 - 1\\ &= \int_0^\infty (2t/c^2)\exp(t/c)^2\mathbb{P}(\{|f| > t\})dt\\ &\le \int_0^\infty (4t/c^2)e^{-\theta t^2}dt\\ &= 2/\theta c^2.\end{aligned}$$

Elementary calculation shows that if $c = (2(e+1)(e-1)^{-1})^{1/2}$ we have $1 + 2/\theta c^2 = e$. Thus we conclude $\|f\|_{\psi_2} \le (2(e+1)(e-1)^{-1})^{1/2}$. By homogeneity, this shows

$$\|f\|_{\psi_2} \le (2(e+1)(e-1)^{-1})^{1/2} sg(f).$$

Lastly the equivalence between $\|f\|_{\psi_2}$ and $\sup_{p\ge1} p^{-1/2}\|f\|_p$ is a particular case of (3.1). □

The equivalence between (ii) and (iv) of Lemma 3.1 can be made more precise, as follows.

Lemma 3.3. *The norm $f \mapsto \|f\|_{\psi_a}$ on L_{ψ_a} is equivalent to $f \mapsto \mathbb{E}\sup_{n\ge1}(\log(n+1))^{-1/a}|f_n|$.*

Proof. Assume $\|f\|_{\psi_a} \le 1$. Then $\mathbb{E}\exp|f|^a \le e$. Let $F = \sup_{n\ge1}(\log(n+1))^{-1/a}|f_n|$. Then $\forall c > 0$

$$\begin{aligned}\mathbb{P}(\{F > c\}) &\le \sum\nolimits_1^\infty \mathbb{P}(\{|f| > c(\log(n+1))^{-1/a}\})\\ &\le \sum\nolimits_1^\infty e\exp(-c^a\log(n+1)\\ &= e\sum\nolimits_1^\infty (n+1)^{-c^a}.\end{aligned}$$

If $c^a > 4$ we have a fortiori

$$\mathbb{P}(\{F > c\}) \le e\sum\nolimits_1^\infty (n+1)^{-2}2^{-c^a/2} \le K2^{-c^a/2},$$

where $K = e\sum_1^\infty (n+1)^{-2}$. From this we derive immediately

$$\mathbb{E}F = \int_0^\infty \mathbb{P}(\{F > c\})dc \le K'$$

where $K' = 4^{1/a} + \int_{4^{1/a}} K2^{-c^a/2}dc$. By homogeneity, this yields $\mathbb{E}F \le K'\|f\|_{\psi_a}$ for any $f \in L_{\psi_a}$.

We now turn to the converse. Assume $\mathbb{E}F \le 1$. Then $\mathbb{P}(\{F \le 2\}) \ge 1/2$, and hence

$$\prod\nolimits_{n\ge1} \mathbb{P}(\{|f| \le 2(\log(n+1))^{1/a}\}) \ge 1/2.$$

But

$$\begin{aligned}&\mathbb{P}(\{|f| \le 2(\log(n+1))^{1/a}\})\\ =\ &1 - \mathbb{P}(\{|f| > 2(\log(n+1))^{1/a}\})\\ \le\ &\exp^{-\mathbb{P}(\{|f|>2(\log(n+1))^{-1/a}\})}\end{aligned}$$

and hence

$$\sum\nolimits_{n\ge1} \mathbb{P}(\{|f| > 2(\log(n+1))^{-1/a}\}) \le \log 2$$

or equivalently

$$\sum\nolimits_{n\ge1} \mathbb{P}(\{\psi_a(|f|/2) > n\}) \le \log 2.$$

But it is classical that for any variable $Z \in L_1$ we have $\mathbb{E}Z \le 1 + \sum_{n\ge1}\mathbb{P}(\{Z > n\})$, so we conclude

$$\mathbb{E}\psi_a(|f|/2) \le 1 + \log 2 \le e,$$

and hence $\|f\|_{\psi_a} \le 2$. By homogeneity, $\|f\|_{\psi_a} \le 2\mathbb{E}F$ for any $f \in L_{\psi_a}$. □

Remark 3.4 (On L_{ψ_a} and the Fourier transform). Let G be a compact Abelian group. Let $f_1, f_2, g_1, g_2 \in L_4(G)$. It is well known that if $|\widehat{f_j}| \le \widehat{g}_j$ on $\widehat{G}$ $(j = 1, 2)$ then

$$\|f_1f_2\|_2 \le \|g_1g_2\|_2.$$

Indeed, this follows from $\|f_1f_2\|_2 = \|\widehat{f_1} * \widehat{f_2}\|_2$, $|\widehat{f_1} * \widehat{f_2}| \le \widehat{g}_1 * \widehat{g}_2$ and again $\|g_1g_2\|_2 = \|\widehat{g}_1 * \widehat{g}_2\|_2$.
Iterating this idea, we find that if $f_1, \cdots, f_m \in L_{2m}(G)$ are such that $|\widehat{f_j}| \le \widehat{g}_j$ on $\widehat{G}$ $(j = 1, \cdots, m)$ we have

$$\|f_1 \cdots f_m\|_2 \le \|g_1 \cdots g_m\|_2.$$

In particular, taking $f_1 = \cdots = f_m = f$ and $g_1 = \cdots = g_m = g$ we find that if $f, g \in L_{2m}(G)$ are such that $|\widehat{f}| \le \widehat{g}$ on $\widehat{G}$, then

$$\|f\|_{2m} \le \|g\|_{2m}.$$

This implies that for any $a > 0$ we have

$$\sup\nolimits_{p\in 2\mathbb{N}} p^{-1/a}\|f\|_p \le \sup\nolimits_{p\in 2\mathbb{N}} p^{-1/a}\|g\|_p.$$

By (3.1), we have

$$\|f\|_{\psi_a} \le C_a\|g\|_{\psi_a},$$

where C_a is a constant depending only on a.

4 Slepian's and Talagrand's Comparison Theorems

A collection of random variable $\{X_s \mid s \in S\}$ on a probability space $(\Omega, \mathbb{P})$ is called Gaussian (resp. subgaussian) if all the variables in its linear span are Gaussian (resp. subgaussian). In this definition, we include in parallel the real and complex case, that we will distinguish if necessary by $\mathbb{R}$-Gaussian or $\mathbb{C}$-Gaussian (resp. $\mathbb{R}$-subgaussian or $\mathbb{C}$-subgaussian).

Convention: To avoid any discussion concerning separability of random processes, for any real valued random process $\{X_s \mid s \in S\}$ in $L_1(\Omega, \mathbb{P})$ by convention, we define the number $\mathbb{E}\sup_{s\in S} X_s$ (possibly $= \infty$) by setting

$$\mathbb{E}\sup_{s\in S} X_s = \sup_{S'\subset S} \mathbb{E}\sup_{s\in S'} X_s,$$

where the sup runs over all *finite* subsets $S' \subset S$.

The following comparison theorem originally due to Slepian is of paramount importance in the theory of Gaussian processes. It was later on refined by various authors. The version we state was popularized by Fernique (see [10]).

Theorem 4.1 (Slepian's comparison principle)**.** *Let $\{X_s \mid s \in S\}$ and $\{Y_s \mid s \in S\}$ be two $\mathbb{R}$-Gaussian processes such that*

$$\forall s, t \in S \quad \|Y_s - Y_t\|_2 \leq \|X_s - X_t\|_2.$$

Then

$$\mathbb{E}\sup_{s\in S} Y_s \leq \mathbb{E}\sup_{s\in S} X_s.$$

Moreover if we also have $\mathbb{E}|Y_s|^2 = \mathbb{E}|X_s|^2$ for all $s \in S$ then for any finite $S' \subset S$

$$\forall c \in \mathbb{R} \quad \mathbb{P}(\{\sup_{s\in S'} Y_s > c\}) \leq \mathbb{P}(\{\sup_{s\in S'} X_s > c\}).$$

We should emphasize that this is a quite non trivial phenomenon, special to Gaussian processes. Indeed, in general a comparison of the covariances is far from implying a comparison of the suprema of the processes.

It is natural to wonder whether a similar comparison theorem holds when Y is merely subgaussian. This turns out to be true, but highly non trivial:

Theorem 4.2 (Talagrand's comparison principle)**.** *Let $\{X_s \mid s \in S\}$ be $\mathbb{R}$-Gaussian process and $\{Y_s \mid s \in S\}$ $\mathbb{R}$-subgaussian. Assume*

$$\forall s, t \in S \quad sg(Y_s - Y_t) \leq \|X_s - X_t\|_2,$$

or equivalently, $\forall x \in \mathbb{R}$ $\forall s, t \in S$,

$$\mathbb{E}\exp x(Y_s - Y_t) \leq \exp(x^2\mathbb{E}|X_s - X_t|^2/2).$$

Then

$$\mathbb{E}\sup_{s\in S} Y_s \leq \tau\mathbb{E}\sup_{s\in S} X_s,$$

where τ is a numerical constant.

The genesis of this result started when Fernique (see [10]) proved his characterization of stationary Gaussian processes with a.s. bounded sample paths. His result implied that if S is a group and if the distribution of $\{X_s \mid s \in S\}$ is invariant under translation (stationarity), then the comparison in Theorem 4.2 holds for any $\mathbb{R}$-subgaussian $\{Y_s \mid s \in S\}$. Later on, Talagrand proved a similar characterization (the so-called majorizing measure condition) of Gaussian processes with a.s. bounded sample paths, without assuming any stationarity. To explain this, let us go back to the stationary case. Roughly, when S is a compact group and $\{X_s \mid s \in S\}$ is stationary the normalized Haar measure on S provides a way to estimate $\mathbb{E}\sup_{s\in S} X_s$. More precisely, $\mathbb{E}\sup_{s\in S} X_s$ is equivalent to the metric entropy integral

$$\int_0^\infty (\log N_X(\varepsilon))^{1/2} d\varepsilon,$$

where $N_X(\varepsilon)$ is the smallest number of a covering of S by open balls of radius ε for the metric $d_X(s,t) = (\mathbb{E}|X_t - X_s|^2)^{1/2}$. (Note that $\log N_X(\varepsilon) = 0$ when ε is larger than the diameter, and the latter is necessarily finite). In the stationary case, when both the Haar measure and d_X are translation invariant, $N_X(\varepsilon)$ is equivalent to $m_G(\{s \mid d_X(s,1) < \varepsilon\})^{-1}$ and hence the latter integral is equivalent to

$$\mathcal{I}_2(X) = \int_0^\infty (\log \frac{1}{m_G(\{s \mid d_X(s,1) < \varepsilon\})})^{1/2} d\varepsilon.$$

When $\mathcal{I}_2(X) < \infty$ it is known (this is a subgaussian variant of Dudley's majorization of Gaussian processes) that all the $\mathbb{R}$-subgaussian processes $\{Y_s \mid s \in S\}$ such that $sg(Y_s - Y_t) \leq d_X(s,t)$ satisfy

$$\mathbb{E}\sup_{s\in S} Y_s \leq \tau'\mathcal{I}_2(X)$$

for some numerical constant τ'. Together with the equivalence $\mathbb{E}\sup_{s\in S} X_s \simeq \mathcal{I}_2(X)$ this leads to Theorem 4.2 assuming X *stationary* $\mathbb{R}$-Gaussian.

For general a.s. bounded Gaussian processes (X_t), Fernique conjectured the existence of a "majorizing measure" that would replace Haar measure. Namely there should exist a probability μ on S such that

$$\mathcal{I}(\mu, X) = \sup_{t\in S} \int_0^\infty (\log \frac{1}{\mu(\{s \mid d_X(s,t) < \varepsilon\})})^{1/2} d\varepsilon < \infty. \quad (4.1)$$

More precisely, for some constant $c > 0$, we should have for any bounded Gaussian processes (X_t)

$$\inf_\mu \mathcal{I}(\mu, X) \leq c\mathbb{E}\sup_{s\in S} X_s \quad (4.2)$$

where the infimum on the left-hand side runs over all probabilities μ on S. In the latter form, the question can be reduced to the case when S is a finite set (with-of course-c independent of S). In his paper [37] (see also [39, §2.4]) Talagrand proved this conjecture. This was a major achievement. He showed that if $\mathbb{E}\sup_{s\in S} X_s \leq 1$ there is a probability measure μ (the so-called majorizing measure) satisfying (4.1). Here again (4.1) also allows one to majorize all the $\mathbb{R}$-subgaussian processes $\{Y_s \mid s \in S\}$ such that $sg(Y_s - Y_t) \leq d_X(s,t)$, namely we have a numerical constant such that $\mathbb{E}\sup_{s\in S} Y_s \leq \tau''\mathcal{I}(\mu, X)$. Thus he obtains Theorem 4.2 as a corollary of his main result, just like in the stationary case. Note that, even though it does not involve majorizing measures, as far as we know the only known proof of Theorem 4.2 uses (4.2) in some form or other. In later work Talagrand chose to reformulate the majorizing measure condition in terms of what he called chainings, and he emphasized the "generic chaining" : he showed that the quantity $\inf_\mu \mathcal{I}(\mu, X)$ that is equivalent (with universal constants independent of X or S) to $\mathbb{E}\sup_{s\in S} X_s$ is similarly equivalent to

$$\inf \sup_{s\in S} \sum\nolimits_{n\geq 0} 2^{n/2} d_X(s, S_n)$$

where the infimum is now taken over all sequences of subsets $S_n \subset S$ with cardinality $|S_n| < 2^{2^n}$ for all n. See [38, 39].

Remark 4.3. For any $\mathbb{R}$-Gaussian process (or any real valued process such that $\{X_s \mid s \in S\}$ and $\{-X_s \mid s \in S\}$ have the same distribution) we have

$$\mathbb{E}\sup_{s\in S} X_s = \mathbb{E}\sup_{s,t\in S} |X_s - X_t|/2.$$

Indeed, $\mathbb{E}\sup_{s,t\in S} |X_s - X_t| = \mathbb{E}\sup_{s,t\in S}(X_s - X_t) = \mathbb{E}\sup_s X_s + \mathbb{E}\sup_{t\in S} -X_t = 2\mathbb{E}\sup_{s\in S} X_s$.

Corollary 4.4. *Let (f_n) be a (real or complex) subgaussian sequence with $sg(\{f_n\}) \leq 1$. Let (g_n) be a normalized i.i.d. $\mathbb{R}$-Gaussian sequence. Let E_g (resp. E_f) be the linear span of (g_n) (resp. (f_n)). Let $u:\ E_g \to E_f$ be the linear operator such that $u(g_n) = f_n$. Then for any n and any $x_1, \cdots, x_n \in E_g$ we have*

$$\mathbb{E}\sup_j |u(x_j)| \leq C_0 \mathbb{E}\sup_j |x_j|, \qquad (4.3)$$

where C_0 is a numerical constant.

Proof. Assume first that (f_n) is $\mathbb{R}$-subgaussian and $sg(\{f_n\}) \leq 1$. Assume the linear spans and u are all in the $\mathbb{R}$-linear sense. Let $y_j = u(x_j)$. Then, since $sg(\{f_n\}) \leq 1$, for any $1 \leq s,t \leq n$ we have $sg(y_s - y_t) \leq \|x_s - x_t\|_2$. Also $sg(y_s) \leq \|x_s\|_2$. A fortiori (see Lemma 1.1) we have $\|y_s\|_2 \leq \|x_s\|_2$. By Theorem 4.2 with $S = \{1, \cdots, n\}$ we have $\mathbb{E}\sup y_s \leq \tau\mathbb{E}\sup x_s$, and also $\mathbb{E}\sup -y_s \leq \tau\mathbb{E}\sup x_s$. Therefore

$$\begin{aligned}\mathbb{E}\sup_{s,t\in S} |y_s - y_t| &= \mathbb{E}\sup_{s,t\in S} y_s - y_t \\ &\leq 2\tau\mathbb{E}\sup x_s \\ &\leq 2\tau\mathbb{E}\sup |x_s|,\end{aligned}$$

and hence

$$\begin{aligned}\mathbb{E}\sup_{s\in S} |y_s| &\leq \mathbb{E}|y_1| + \mathbb{E}\sup_{s\in S} |y_s - y_1| \\ &\leq \|y_1\|_2 + 2\tau\mathbb{E}\sup |x_s| \\ &\leq \|x_1\|_2 + 2\tau\mathbb{E}\sup |x_s|\end{aligned}$$

and since $\|x_1\|_2 \leq (2/\sqrt{\pi})\|x_1\|_1$ we obtain the announced result with $C_0 \leq 2/\sqrt{\pi} + 2\tau$.
Now assume (f_n) is $\mathbb{C}$-subgaussian but with u, E_g, E_f still with respect to $\mathbb{R}$-linearity, the first part of the proof can be applied separately to the real and imaginary parts of (f_n), then the triangle inequality yields (4.3) with a double constant. Lastly, if E_g is the $\mathbb{C}$-linear span and u is $\mathbb{C}$-linear, if $x = \sum(a_k + ib_k)g_k$ we have $u(x) = u(\sum a_k g_k) + iu(\sum b_k g_k)$ and hence

$$|u(x)| \leq |u(\sum a_k g_k)| + |u(\sum b_k g_k)|$$

and again the first part of the proof allows us to conclude that (4.3) holds. □

We will need one more characterization of subgaussian sequences, for which the next definition will be very useful.

Definition. Consider families $\{\varphi_n\} \subset L_1(T, m)$, and $\{\gamma_n\} \subset L_1(T', m')$ indexed by the same index set I. We say that (φ_n) is C-dominated by (γ_n) if there is an operator $u:\ L_1(m') \to L_1(m)$

$$\text{with } \|u\| \leq C \text{ such that } \ u(\gamma_n) = \varphi_n\ \forall n \in I. \qquad (4.4)$$

Proposition ([21], see also [31])**.** *The sequence (φ_n) is C-dominated by (γ_n) iff for any N and any $f_1, \cdots, f_N$ in the linear span of $\{\gamma_n\}$ of the form $f_i = \sum_j a_{ij}\gamma_j$, the associated $\widetilde{f}_i = \sum_j a_{ij}\varphi_j$ satisfy*

$$\|\sup_i |\widetilde{f}_i|\|_1 \leq C\|\sup_i |f_i|\|_1. \qquad (4.5)$$

Proof. Let E be the linear span of $\{\gamma_n\}$. Assume (4.5). Our assumption implies a fortiori that

$$\|\sum\nolimits_j a_j\varphi_j\|_1 \leq \|\sum\nolimits_j a_j\gamma_j\|_1.$$

Therefore we can unambiguously define

$$u\colon\ E \to L_1(T', m'),$$

by setting $u(\sum_j a_j\gamma_j) = \sum_j a_j\varphi_j$. Our assumption then means that

$$\|\sup |u(f_i)|\|_1 \leq C\|\sup |f_i|\|_1$$

for any finite set (f_i) in E. The content of the Proposition is that u admits an extension $\widetilde{u}:\ L_1(m) \to L_1(m')$ with $\|\widetilde{u}\| \leq C$. We will reduce the proof to the following claim. Assume that (T', m') is an atomic measure space and that T' is partitioned into a finite set of disjoint atoms $A_1, \cdots, A_n$. If for any $f_1, \cdots, f_n \in E$ we have

$$|\sum\nolimits_1^n \int_{A_i} u(f_i)dm'| \leq C\|\sup |f_i|\|_1$$

then u admits an extension $\widetilde{u}:\ L_1(m) \to L_1(m')$ with $\|\widetilde{u}\| \leq C$.
Let us first accept this claim. Note that

$$|\sum\nolimits_1^n \int_{A_i} u(f_i)dm'| \leq \|\sup |u(f_i)|\|_1.$$

Thus the claim is nothing but the Proposition in the case when (T', m') is atomic with finitely many atoms. Thus using the directed net of finite subalgebras of (T', m') one can get an extension

$$\widetilde{u}: \ L_1(T,m) \to L_1(T',m')^{**}$$

with norm $\leq C$, and then, using the fact that there is a projection of norm 1 from $L_1(T',m')^{**}$ to $L_1(T',m')$ (see Remark 4.5), we get a $\widetilde{u}$ with range into $L_1(T',m')$. Thus it suffices to check the claim. This is an application of Hahn-Banach. Let $\mathcal{E} = E^n$ equipped with the norm induced by $L_1(m;\ell_n^\infty)$, or more explicitly for all $f = (f_1,\cdots,f_n) \in \mathcal{E}$ we set $\|(f_1,\cdots,f_n)\|_{\mathcal{E}} = \|\sup|f_i|\|_1$. Let $\xi \in \mathcal{E}^*$ be the linear form defined for all $f \in \mathcal{E}$ by

$$\xi(f) = \sum\nolimits_1^n \int_{A_i} u(f_i)dm'.$$

By our assumption $\|\xi\|_{\mathcal{E}^*} \leq C$. Let $\widetilde{\xi} \in L_1(m;\ell_n^\infty)^*$ be the Hahn-Banach extension of ξ, such that for all $F = (F_1,\cdots,F_n) \in L_1(m)^n$

$$|\widetilde{\xi}(F)| \leq C\|\sup|F_i|\|_1.$$

Obviously we have $\Phi_1,\cdots,\Phi_n$ in $L_\infty(m)$ such that $\|\sum|\Phi_i|\|_\infty \leq C$ and such that $\widetilde{\xi}(F) = \sum\int\Phi_i F_i dm$. Note that for any $f \in \mathcal{E}$ we have

$$\sum\int \Phi_i f_i dm = \xi(f) = \sum\nolimits_1^n \int_{A_i} u(f_i)dm'.$$

Let then $\widetilde{u}(x) = \sum_i 1_{A_i} m'(A_i)^{-1}(\int\Phi_i x dm)$. Clearly $\|\widetilde{u}\| \leq \|\sum|\Phi_i|\|_\infty \leq C$, and (recalling that $u(x) \in \text{span}[1_{A_i}]$) we have

$$\begin{aligned}\forall x \in E \quad \widetilde{u}(x) &= \sum\nolimits_i 1_{A_i} m'(A_i)^{-1} \int_{A_i} u(x)dm' \\ &= \sum\nolimits_i 1_{A_i} u(x) \\ &= u(x).\end{aligned}$$

This proves the claim. □

Remark 4.5. Let $(T,\mathcal{A},m)$ be a countably generated probability space, so that there is an increasing filtration $(\mathcal{A}_n)$ of finite σ-subalgebras whose union generates $\mathcal{A}$. The classical fact that there is a norm 1-projection $P: \ L_1(T,m)^{**} \to L_1(T,m)$ is easy to prove using martingales as follows. Just observe that any $f \in L_1(T,\mathcal{A},m)^{**} = L_\infty(T,\mathcal{A},m)^*$ induces by restriction to $L_\infty(T,\mathcal{A}_n,m)$ a sequence (f_n) with $f_n \in L_1(T,\mathcal{A}_n,m) = L_\infty(T,\mathcal{A}_n,m)^*$. It is easy to see that (f_n) is a martingale bounded in $L_1(T,\mathcal{A},m)$ by the norm of f in $L_1(T,\mathcal{A},m)^{**}$. By the martingale convergence theorem, (f_n) converges a.s. to a limit $f_\infty \in L_1(T,\mathcal{A},m)$, with $\|f_\infty\|_1 \leq \|f\|$. In general the convergence does not hold in $L_1(T,\mathcal{A},m)$. However if our original $f \in L_1(T,\mathcal{A},m)^{**}$ happens to be in $L_1(T,\mathcal{A},m)$ then the convergence holds in $L_1(T,\mathcal{A},m)$ and $f_\infty = f$. Thus if we set $P(f) = f_\infty$, we obtain the desired projection. See our recent book [32] for basic martingale convergence theorems and for more information of the many connections of martingale theory with Banach space theory and harmonic analysis.

We denote by (g_n) an i.i.d. sequence of normalized $\mathbb{R}$-Gaussian random variables on some probability space $(\Omega,\mathbb{P})$. Given a sequence $\{\varphi_n\} \subset L_1(T,m)$, we denote by $\{\varphi_{n,k}\} \subset L_1(T^{\mathbb{N}}, m^{\otimes\mathbb{N}})$ the family defined by

$$\forall t \in T^{\mathbb{N}} \quad \varphi_{n,k}(t) = \varphi_n(t_k).$$

Note that the definition of subgaussian (Definition 1.8) shows that if (φ_n) is subgaussian, $\{\varphi_{n,k}\}$ is also subgaussian with $sg(\{\varphi_{n,k}\}) = sg(\{\varphi_n\})$.

Concerning Definition 4: we will need to consider (φ_n) such that $\{\varphi_{n,k}\}$ is C-dominated by $(g_{n,k})$. Of course the reader will note that the sequences $(g_{n,k})$ and (g_n) have the same distribution, so we will say (abusively) in this case that $\{\varphi_{n,k}\}$ is C-dominated by (g_n).

We will denote by $C_{dom}(\{\varphi_n\})$ the smallest C such that $\{\varphi_n\}$ is C-dominated by (g_n).

Proposition. *There is a numerical constant c_1 such that any C-subgaussian sequence $\{\varphi_n\} \subset L_1(T,m)$ is c_1C-dominated by (g_n).*

More precisely, assuming $\mathbb{E}\varphi_n = 0$ for all n, the following are equivalent.

- *(i) For some C the sequence $\{\varphi_n\} \subset L_1(T,m)$ is C-subgaussian.*
- *(ii) For some C' the sequence $\{\varphi_{n,k}\}$ is C'-dominated by (g_n).*

Moreover, we have

$$c_1^{-1}C_{dom}(\{\varphi_{n,k}\}) \leq sg(\{\varphi_n\}) \leq c_2 C_{dom}(\{\varphi_{n,k}\})$$

where c_2 is another positive constant independent of $\{\varphi_n\}$.

Sketch. The first assertion is a consequence of Talagrand's comparison principle together with Proposition 4. From this we deduce

$$C_{dom}(\{\varphi_n\}) \leq c_1 sg(\{\varphi_n\}).$$

As we already observed, $sg(\{\varphi_n\})$ is equal to $sg(\{\varphi_{n,k}\})$. Thus

$$C_{dom}(\{\varphi_{n,k}\}) \leq c_1 sg(\{\varphi_{n,k}\}) = c_1 sg(\{\varphi_n\}),$$

and hence (i) ⇒ (ii).

Conversely, if (ii) holds, for any $f = \sum x_n\varphi_n$ with $\sum|x_n|^2 = 1$ we have (with the notation in Lemma 3.3)

$$\begin{aligned}&\mathbb{E}\sup\nolimits_{k\geq 1}(\log(k+1))^{-1/2}|f_k| \\ &\qquad \leq C_{dom}(\{\varphi_{n,k}\})\mathbb{E}\sup\nolimits_{k\geq 1}(\log(k+1))^{-1/2}|g_k|\end{aligned}$$

and hence by Lemma 3.3 $\|f\|_{\psi_2} \le c_2' C_{dom}(\{\varphi_{n,k}\})$ for some numerical constant c_2'. By Lemma 3.2 we obtain $sg(f) \le c_2 C_{dom}(\{\varphi_{n,k}\})$ for some numerical constant c_2, or equivalently

$$sg(\{\varphi_n\}) \le c_2 C_{dom}(\{\varphi_{n,k}\}),$$

which proves (ii) ⇒ (i). □

5 Subgaussian sequences in harmonic analysis

More subgaussian examples come from Fourier analysis. Let $0 < k(0) < k(1) < \cdots < k(n) < \cdots$ be a sequence of integers such that

$$\inf_n\{k(n+1)/k(n)\} > 1. \tag{5.1}$$

Such sequences are called "Hadamard lacunary". The simplest example is the sequence $k(n) = 2^n$. The associated sequence

$$f_n = \exp(ik(n)t)$$

on $[0, 2\pi], dt/2\pi$ is subgaussian. We will check this in Proposition 5. Of course the real (or the imaginary) parts also form a subgaussian sequence. Although these are not independent random variables on the unit circle, it turns out that they behave in many ways as independent ones. For instance, while the sequence $f_n(t) = \sin(2^n t)$ is not independent, the ±1-valued sequence formed of its signs $(\operatorname{sign}(f_n(t)))$ is stochastically independent.

For any subset $\Lambda \subset \mathbb{Z}$ not containing 0 we say that Λ is subgaussian if the system

$$\widetilde{\Lambda} = \{\exp(ikt) \mid k \in \Lambda\}$$

is subgaussian. We set by convention

$$sg(\Lambda) = sg(\widetilde{\Lambda}).$$

More generally we will consider subsets Λ of a discrete Abelian group $\widehat{G}$. Then Λ is formed of continuous characters on the dual group G, which is a compact Abelian group equipped with its normalized Haar measure m_G. In that case $sg(\Lambda)$ is the subgaussian constant of the family $\{\gamma \mid \gamma \in \Lambda\}$ viewed as random variables on (G, m_G).

The sequence $\{2^n\}$ is close to independent in the following sense:

Definition. A subset $\Lambda \subset \mathbb{Z}$ is called quasi-independent if the sums $\sum_{n\in A} n$ are distinct integers when A runs over all the finite subsets of Λ.

Remark 5.1. Any sequence $\{k(n)\}$ such that $k(n) > \sum_{j<n} k(j)$ (for example $k(n) = 2^n$) is clearly quasi-independent.

A finite set $\Lambda \subset \mathbb{Z}$ is quasi-independent iff

$$\int \prod_{n\in\Lambda}(1 + e^{int} + e^{-int})dt/2\pi = 1,$$

or equivalently iff for some $0 < \delta \le 1$

$$\int \prod_{n\in\Lambda}(1 + \delta(e^{int} + e^{-int}))dt/2\pi = 1.$$

Indeed, the preceding integral can be rewritten as $1 + \delta a_1 + \delta^2 a_2 + \cdots + \delta^{|\Lambda|} a_{|\Lambda|}$ where $a_1, a_2, \cdots$ are non-negative integers.

From now on let $dm(t) = dt/2\pi$ on $[0, 2\pi]$. We have then

Proposition. *Any quasi-independent sequence $\Lambda \subset \mathbb{Z}$ is subgaussian on $([0,1], dt/2\pi)$ with constant ≤ 2. More generally, any Hadamard lacunary sequence is subgaussian.*

Proof. We may assume Λ finite and $0 \notin \Lambda$ For any $z = (z_k) \in \mathbb{T}^\Lambda$ let

$$F_z = \prod_{n\in\Lambda}(1 + \Re(\bar{z}_n e^{int})).$$

Note that if $k = \sum_{n\in A} n$ we have $\widehat{F_z}(k) = \prod_{n\in A}(\bar{z}_n/2)$. Moreover $F_z \ge 0$ and $\int F_z dm = 1$.
Let $f_z = \sum_{n\in\Lambda} z_n x_n e^{int}$ and $f = \sum_{n\in\Lambda} x_n e^{int}$. Then $\Re(f_z) * F_z = \Re(f)/2$. Therefore by the convexity of the exponential function

$$\int e^{\Re(f)/2} dm \le \int (\int F_z(s) e^{\Re(f_z(t-s))} dm(s)) dm(t)$$

and by Fubini and the translation invariance of m this implies

$$\begin{aligned}\int e^{\Re(f)/2} dm &\le \int F_z(s) dm(s) \int e^{\Re(f_z(t))} dm(t)\\ &= \int e^{\Re(f_z(t))} dm(t).\end{aligned}$$

We now average the right hand side over z with respect to the normalized Haar measure on the group $G = \mathbb{T}^\Lambda$. By Fubini this gives us

$$\begin{aligned}\int e^{\Re(f)/2} dm &\le \int e^{\Re(f_z(t))} dm(t) dm_G(z)\\ &= \int (\int e^{\Re(f_z(t))} dm_G(z)) dm(t)\end{aligned}$$

and since we already know that $sg(\{z_n\}) \le 1$ (or equivalently $sg(\{\bar{z}_n\}) \le 1$) we find

$$\int e^{\Re(f)/2} dm \le \exp(\sum |x_n|^2/2),$$

and we conclude by homogeneity that

$$sg(\{e^{int} \mid n \in \Lambda\}) \le 2.$$

It is easy to check that a Hadamard lacunary sequence is a finite union of sequences $(k(n))$ satisfying $k(n+1)/k(n) \ge 2$ for all n. Since such sequences are clearly quasi-independent (see Remark 5.1) the second assertion follows. □

More generally, let us replace $\mathbb{T}$ by a compact Abelian group G equipped with its normalized Haar measure m_G. The dual group $\widehat{G}$ is the discrete group formed of all the continuous characters on G. A character is a homomorphism $\gamma : G \to \mathbb{T}$. The group operation on $\widehat{G}$ is the pointwise product of characters. When $G = \mathbb{T}$ the characters are all of the form $\gamma_n(z) = z^n$ ($z \in \mathbb{T}$) for some $n \in \mathbb{Z}$. The correspondence $\gamma_n \leftrightarrow n$ allows us to identify $\widehat{\mathbb{T}}$ with $\mathbb{Z}$ as discrete groups (pointwise multiplication on $\widehat{\mathbb{T}}$ corresponds to addition on $\mathbb{Z}$).

Remark 5.2. The implication quasi-independent $\Rightarrow$ subgaussian remains clearly valid with the same proof for a subset Λ of any discrete group $\widehat{G}$.

Theorem 5.3. *Let $(f_1, \cdots f_n)$ be subgaussian on a probability space (T, m) with $sg(\{f_k\}) \leq s$. Assume that $\|f_k\|_2 = 1$ and $\|f_k\|_\infty \leq C$. Then for any $0 < \delta < 1/C$ there is a subset $\mathcal{T} \subset T$ with*

$$\log |\mathcal{T}| \geq n(1 - \delta C)^2/(2s^2C^2),$$

such that for any $x \neq y \in \mathcal{T}$ we have

$$(\textstyle\sum_1^n |f_k(x) - f_k(y)|^2)^{1/2} > \delta\sqrt{n}.$$

Proof. Let $\mathcal{T}$ be a maximal subset with this property. Then for any $x \in T$ there is $y \in \mathcal{T}$ such that $(\sum_1^n |f_k(x) - f_k(y)|^2)^{1/2} \leq \delta\sqrt{n}$, and hence

$$\begin{aligned}\textstyle\sum_1^n |f_k(x)|^2 &= \textstyle\sum_1^n \Re(f_k(x)\overline{f_k(x)}) \\ &\leq \textstyle\sum_1^n \Re(f_k(x)\overline{f_k(y)}) + \delta n C.\end{aligned}$$

Therefore for any $\lambda > 0$

$$\begin{aligned}&\exp \lambda n = \exp \lambda \textstyle\sum_1^n \int |f_k|^2 dm \\ &\leq \int \exp \lambda \textstyle\sum_1^n |f_k(x)|^2 m(dx) \\ &\leq e^{\lambda\delta nC} \int \exp(\lambda \sup_{y\in\mathcal{T}} \textstyle\sum_1^n \Re(f_k(x)\overline{f_k(y)}))m(dx) \\ &\leq e^{\lambda\delta nC} \textstyle\sum_{y\in\mathcal{T}} \int \exp(\lambda \textstyle\sum_1^n \Re(f_k(x)\overline{f_k(y)}))m(dx) \\ &\leq e^{\lambda\delta nC}|\mathcal{T}| \exp(\lambda^2 s^2 nC^2/2).\end{aligned}$$

Therefore

$$|\mathcal{T}| \geq \exp n(\lambda(1 - \delta C) - \lambda^2 s^2 C^2/2).$$

Choosing $\lambda = (s^2C^2)^{-1}(1 - \delta C)$ (to maximize the last expression) we obtain the announced inequality. □

Remark 5.4. Note that in the preceding proof instead of $sg(\{f_k\}) \leq s$ it suffices to assume $sg(\sum_1^n x_k f_k) \leq s\sqrt{n} \sup |x_k|$ for any $x_k \in \mathbb{C}$.

In Theorem 5.3, we have obviously $|T| \geq |\mathcal{T}|$. In particular:

Corollary 5.5. *Let $(f_1, \cdots f_n)$ be subgaussian characters on a finite Abelian group G with $sg(\{f_k\}) \leq s$. Then for any $0 < \delta < 1$*

$$\log |G| \geq (1 - \delta)^2/2s^2.$$

Corollary 5.6. *In the situation of Theorem 5.3, assume in addition that $(f_1, \cdots f_n)$ are continuously differentiable functions on $([0, 2\pi], dt/2\pi)$. Then*

$$\begin{aligned}&n^{-1/2}\|(\textstyle\sum |f_k'|^2)^{1/2}\|_\infty \geq \\ &\qquad \frac{\delta}{2\pi}\left(\exp(n(1 - \delta C)^2/(2s^2C^2)) - 1\right).\end{aligned}$$

Proof. Let $L = n^{-1/2}\|(\sum_1^n |f_k'|^2)^{1/2}\|_\infty$ We have for any $x, y \in [0, 2\pi]$

$$(\textstyle\sum_1^n |f_k(x) - f_k(y)|^2)^{1/2} \leq n^{1/2}L|x - y|.$$

Therefore for any $x \neq y \in \mathcal{T}$

$$|x - y| \geq \delta/L.$$

But obviously, we cannot find more that $1 + 2\pi L/\delta$ points in $[0, 2\pi]$ with mutual distance $\geq \delta/L$. Thus we conclude $2\pi L/\delta \geq |\mathcal{T}| - 1$ □

Corollary 5.7. *If $\Lambda \subset [1, \cdots, N]$ (or if Λ is included in an arithmetic progression of length N) and $sg(\{e^{int} \mid n \in \Lambda\}) \leq s$, then*

$$\log(\frac{2\pi N}{\delta} + 1) \geq |\Lambda|(1 - \delta)^2/2s^2.$$

Proof. The case of an arithmetic progression of length N can be reduced to $[1, \cdots, N]$. For $f_k = e^{ik(n)t}$ with $1 \leq k(n) \leq N$ we have $L \leq N$. □

Remark 5.8. If $\Lambda = \{2^k \mid 1 \leq 2^k \leq N\}$ then $\log N \approx |\Lambda|$; so the logarithmic growth rate for the intersection of a subgaussian set with any arithmetic progression of length N given by Corollary 5.7 is essentially optimal.

Remark 5.9. Let $\Lambda_1 = \{f_n\}$ and $\Lambda_2 = \{h_n\}$ be two subgaussian families of functions on the same probability space. Then the union $\Lambda_1 \cup \Lambda_2$ is subgaussian. This follows from (1.10).

6 Subgaussian sets of integers, arithmetic characterization

We will now describe the existing arithmetic characterization of subgaussian sets of integers and, in the next section, the main open problem concerning them.

For any finite set $\Lambda \subset \mathbb{Z}$ or more generally $\Lambda \subset \widehat{G}$ (here $\widehat{G}$ is any discrete Abelian group denoted additively), let

$$R(\Lambda) = \{\xi \in \{-1, 0, 1\}^\Lambda \mid \textstyle\sum_{n\in\Lambda} \xi_n n = 0\}.$$

In other words $R(\Lambda)$ is the set of relations with coefficients in $\{-1,0,1\}$ satisfied by Λ. Note that Λ is quasi-independent iff $|R(\Lambda)|=1$. The number $R(\Lambda)$ is related to Fourier series by the following obvious identity, valid for any finite subset $A\subset\Lambda$

$$R(A)=\int\prod\nolimits_{n\in A}(1+e^{int}+e^{-int})dm(t). \qquad (6.1)$$

The number $N(k,m,n)$ introduced in the next statement appears in the theory of constant weight codes, see Remark 6.3 below.

Lemma 6.1. *Let $k<m<n$ be integers. As usual let $[n]=\{1,\cdots,n\}$. Let $N(k,m,n)\geq 1$ be the largest possible cardinal of a family $\mathcal{T}$ of subsets of $[n]$ such that*

$$\forall t\in\mathcal{T}\quad |t|=m \text{ and } \forall s\neq t\in\mathcal{T}\quad |s\cap t|\leq k. \qquad (6.2)$$

Let $A\subset\mathbb{Z}$ be a subset with $|A|=n$. If $R(A)<N(k,m,n)$, then A contains a quasi-independent subset $B\subset A$ with

$$|B|\geq m-k.$$

Proof. Since A and $[n]$ are in bijection, we may assume that $\mathcal{T}$ is a family of subsets of A. For any $t\in\mathcal{T}$ consider a maximal subset $r_t\subset t$ that supports a relation, i.e. for $r=r_t$ there exists $(\xi_n)\in\{-1,1\}^r$ such that $\sum\xi_n n=0$ and there is no larger subset of t satisfying this. We claim that for some t we must have $|r_t|\leq k$. Otherwise, $|r_t|>k$ for all t. But since $|s\cap t|\leq k$ for all $s\neq t$, the mapping $t\mapsto r_t$ must be one to one. To each r_t we can associate (by adding several zeros) a relation $\xi^t\in\{-1,0,1\}^A$ such that $\sum\xi^t_n n=0$ with support r_t. Obviously $t\mapsto\xi^t$ is also one to one. Thus we obtain $|\mathcal{T}|\leq|R(A)|$, contradicting our assumption that $R(A)<N(k,m,n)$. This proves our claim. Now choose t so that $|r_t|\leq k$. Let $B=t\setminus r_t$. We have $|B|\geq m-k$ and the maximality of $r_t\subset t$ implies that there cannot be any nontrivial relation with coefficients ±1 supported inside B. In other words B is quasi-independent. □

Lemma 6.2. *Assuming that $3n/8, n/2$ are integers, we have*

$$N(3n/8,n/2,n)\geq c'\exp(n/17), \qquad (6.3)$$

where $c'>0$ is independent of n.

Proof. Let Q be the uniform probability over all the 2^n subsets of $[n]$. Let $\mathcal{T}$ be a maximal family of subsets satisfying (6.2). Then for any $A\subset[n]$ with $|A|=m$ and $A\notin\mathcal{T}$ there is $t\in\mathcal{T}$ such that $|A\cap t|>k$ (otherwise we could add A to $\mathcal{T}$ contradicting its maximality). Actually, if $A\in\mathcal{T}$, then $t=A$ trivially satisfies $|A\cap t|=m>k$. Therefore

$$\{A\mid|A|=m\}\subset\cup_{t\in\mathcal{T}}\{A\mid|A|=m,|A\cap t|>k\}$$

and hence

$$Q(\{A\mid|A|=m\})\leq|\mathcal{T}|\sup\nolimits_{t\in\mathcal{T}}Q(\{A\mid|A|=m,\\ |A\cap t|>k\}). \qquad (6.4)$$

Of course, whenever $|t|=m$, the numbers $Q(\{A\mid|A|=m,|A\cap t|>k\})$ are all the same and hence $Q(\{A\mid|A|=m,|A\cap t|>k\})=Q(\{A\mid|A|=m,|A\cap[m]|>k\})$. By an easy counting argument, the cardinal of $\{A\mid|A|=m,|A\cap[m]|>k\}$ is equal to $\sum_{k<j\leq m}\binom{m}{j}\binom{n-m}{m-j}$. Although we could use combinatorics, we prefer to use probability to estimate this number. Let (ε_j) be in $\{-1,1\}^n$ and let P be the uniform probability on $\{-1,1\}^n$. We have a $1-1$ equivalence between P and Q using the correspondence $\varepsilon=(\varepsilon_j)\mapsto A=\{j\mid\varepsilon_j=1\}$. Note $|A|=\sum(\varepsilon_j+1)/2$. Let $S_n=\sum_1^n\varepsilon_j$ so that $|A|=(S_n+n)/2$ and $|A\cap[m]|=(S_m+m)/2$. Thus (6.4) implies

$$\begin{aligned}P(\{S_n=2m-n\})&\leq|\mathcal{T}|P(\{(S_m+m)/2>k\})\\&=|\mathcal{T}|P(\{S_m>2k-m\}). \qquad (6.5)\end{aligned}$$

By a well known bound there is a positive number $c_0>0$ (in fact $c_0=1/\sqrt{2}$) so that assuming n even $\binom{n}{n/2}\geq c_0 2^n/\sqrt{n}$. Thus assuming $n=2m$ and $2k-m=m/2$ we find by (6.5) (using (1.13) and (1.5))

$$\begin{aligned}c_0/\sqrt{n}&\leq|\mathcal{T}|\exp-((2k-m)^2/2m)\\&\leq|\mathcal{T}|\exp-m/8\\&\leq|\mathcal{T}|\exp-n/16,\end{aligned}$$

and we obtain $N(3n/8,n/2,n)\geq(c_0/\sqrt{n})\exp(n/16)$, from which (6.3) follows a fortiori. □

Remark 6.3. The number $N(k,m,n)$ introduced in Lemma 6.1 appears in the theory of constant weight codes where it is denoted by $A(n,2(m-k),m)$. A code word is a sequence of 0's and 1's, its length is the number of 0's and 1's, and its weight is the number of 1's. The Hamming distance between any two such words is the number of places where they differ. Thus $N(k,m,n)$ is equal to the maximal number of code words of length n with weight m and mutual Hamming distance at least $2(m-k)$. The simple packing argument used for Lemma 6.2 is a variant of a famous estimate known in Coding Theory as the Gilbert-Varshamov bound, adapted to the weight m case. It is known (this seems to be in the coding folklore) that if $m=[an]$, $k=[bn]$ with $0<b<a^2$ and $0<a\leq1/2$ then (assuming $n\to\infty$) we have an exponential lower bound $N(k,m,n)\geq 2^{\delta n}$ for some $\delta=\delta(a,b)>0$. The proof of Lemma 6.2 can be modified to yield that. It seems however that no sharp formula is known for $\delta=\delta(a,b)>0$. See [26, chap. 17, §2] for more on this vast subject. I am grateful to Noga Alon for the information and references used in the present remark.

Lemma 6.4. *Assume again that $3n/8, n/2$ are integers. If $|A|=n$ and $|R(A)|<c'\exp(n/17)$ then $\exists B\subset A$ quasi-independent with $|B|\geq n/8$.*

Proof. This is immediate from the preceding two Lemmas. □

Theorem 6.5. *Let $\Lambda \subset \mathbb{Z} \setminus \{0\}$ or more generally $\Lambda \subset \widehat{G} \setminus \{0\}$ ($\widehat{G}$ any discrete Abelian group). The following are equivalent:*

(i) *Λ is subgaussian.*

(ii) *There is $\delta > 0$ such that any finite $A \subset \Lambda$ contains a quasi-independent subset $B \subset A$ with $|B| \geq \delta|A|$.*

(iii) *There is $\delta > 0$ and $s > 0$ such that any finite $A \subset \Lambda$ contains a (subgaussian) subset $B \subset A$ with $|B| \geq \delta|A|$ and $sg(B) \leq s$.*

(iii)' *For any $0 < \delta < 1$ there is $s > 0$ such that any finite $A \subset \Lambda$ contains a (subgaussian) subset $B \subset A$ with $|B| \geq \delta|A|$ and $sg(B) \leq s$.*

(iv) *There is a constant C such that for any finite subset $A \subset \Lambda$ we have*

$$sg(\Re(\textstyle\sum_{n\in A} e^{int})) \leq C|A|^{1/2}.$$

Proof. Assume (i). Then there is C such that for any finite subset $A \subset \Lambda$ with $|A| = n$ the function

$$S_A(t) = \Re(\textstyle\sum_{k\in A} e^{ikt}) = \sum_{k\in A} \cos(kt)$$

is subgaussian with $sg(S_A) \leq C|A|^{1/2}$. Then for any $0 < \delta < 1$ we have

$$\begin{aligned}\int \textstyle\prod_{k\in A}(1+\delta\cos(kt))dm(t) &\leq \int \exp(\delta S_A)dm(t)\\ &\leq \exp(C\delta^2 n/2).\end{aligned}$$

Let $(\delta_k)_{k\in A}$ be an i.i.d. family of $\{0,1\}$-valued variables with $\mathbb{P}(\{\delta_k = 1\}) = \delta/2$. Let $A(\omega) = \{k \mid \delta_k(\omega) = 1\}$. Then

$$\prod_{k\in A(\omega)}(1 + e^{ikt} + e^{-ikt}) = \prod_{k\in A}(1 + \delta_k(\omega)(e^{ikt} + e^{-ikt}))$$

and hence

$$\begin{aligned}\mathbb{E}\int &\textstyle\prod_{k\in A(\omega)}(1 + e^{ikt} + e^{-ikt})dm(t)\\ &= \int \textstyle\prod_{k\in A}(1+\delta\cos(kt))\\ &\leq \exp(C\delta^2 n/2).\end{aligned}$$

In other words

$$\mathbb{E}|R(A(\omega))| \leq \exp(C\delta^2 n/2). \qquad (6.6)$$

But we also have $|A(\omega)| - \delta n/2 = \sum_{k\in A}(\delta_k - \mathbb{E}\delta_k)$, and hence by well known bounds for a sum of independent mean 0 variables with values in $[-1,1]$ (indeed a very particular case of Theorem 1.2 with $d_n = \delta_n - \mathbb{E}\delta_n$ tells us that $sg(\sum_{k\in A}(\delta_k - \mathbb{E}\delta_k)) \leq n^{1/2}$ then we may use (1.5))

$$\begin{aligned}\forall c > 0 \quad &\mathbb{P}(\{|A(\omega)| - \delta n/2 < -c\})\\ &= \mathbb{P}(\{\textstyle\sum_{n\in A}(\delta_n - \mathbb{E}\delta_n) < -c\})\\ &\leq \exp(-c^2/2n).\end{aligned}$$

Therefore

$$\mathbb{P}(\{|A(\omega)| - \delta n/2 < -\delta n/4\}) \leq \exp(-\delta^2 n/32),$$

and hence

$$\mathbb{P}(\{|A(\omega)| \geq \delta n/4\}) \geq 1 - \exp(-\delta^2 n/32).$$

By (6.6)

$$\mathbb{P}(\{|R(A(\omega))| \leq 2\exp(C\delta^2 n/2)\}) \geq 1/2.$$

Assume

$$1/2 + 1 - \exp(-\delta^2 n/32) > 1. \qquad (6.7)$$

Then for some ω we have both $|A(\omega)| \geq \delta n/4$ and $|R(A(\omega))| \leq 2\exp(C\delta^2 n/2)$, and hence

$$|R(A(\omega))| \leq 2\exp(2C\delta|A(\omega)|).$$

We now choose $\delta = \delta_C$ so that $2C\delta_C = 1/18 < 1/17$. Then $|R(A(\omega))| \leq 2\exp(|A(\omega)|/18)$. Note $|A(\omega)| \geq \delta_C n/4$. Therefore there is clearly a large enough number N (depending only on C) such that for all $n \geq N$ both (6.7) and (for the ω we select)

$$2\exp(|A(\omega)|/18) < c'\exp(|A(\omega)|/17)$$

hold, and hence

$$|R(A(\omega))| < c'\exp(|A(\omega)|/17).$$

By Lemma 6.4 this implies that $A(\omega)$ contains a quasi-independent subset B with $|B| \geq |A(\omega)|/8 \geq \delta_C n/32$. (We ignore the requirement that $3|A(\omega)|/8$, $|A(\omega)|/2$ be integers, which is easy to bypass by replacing $A(\omega)$ by a maximal subset with cardinal dividable by 8.) This proves (ii) since the sets with $n \leq N$ are easily treated by adjusting the number δ appearing in (ii) small enough.

(ii) ⇒ (iii) follows from Proposition 5.

Assume (iii). Let $|A| = n$. Let $B \subset A$ be given by (iii), i.e. $sg(B) \leq s$ and $|B| \geq \delta n$. We may apply (iii) again to $A \setminus B$. This gives us $B_1 \subset A \setminus B$ with $sg(B_1) \leq s$ and $|B_1| \geq \delta|A \setminus B|$. Now let $B' = B \cup B_1$. We have $|B'| \geq (\delta + \delta(1-\delta))n$ and, by Remark 5.9 and (1.10), also $sg(B') \leq 2s$. Thus we have improved δ from the value δ to $\delta_1 = \delta + \delta(1-\delta)$. Iterating this process, we easily obtain (iii)'

Assume (iii)'. Let $C(n)$ be the smallest constant C such that $sg(S_A) \leq C\sqrt{|A|}$ for all subsets $A \subset \Lambda$ with $\leq n$ elements. Let $|A| \leq n$. We fix $0 < \delta < 1$ suitably close to 1 (to be determined). Let $B \subset A$ be given by (iii)', so that $sg(S_B) \leq s\sqrt{|B|}$ and $|B| \geq \delta|A|$. We have obviously by definition of $C(n)$ $sg(S_{A\setminus B}) \leq C(n)\sqrt{n(1-\delta)}$. By (1.10),

$$\begin{aligned}sg(S_A)^2 &\leq 2(s^2|B| + C(n)^2|A|(1-\delta))\\ &\leq 2s^2|A| + 2(1-\delta)C(n)^2|A|,\end{aligned}$$

which implies

$$C(n)^2 \leq 2s^2 + 2(1-\delta)C(n)^2.$$

Thus if δ is chosen so that $\delta_1 = 2(1-\delta) < 1$ we conclude

$$C(n)^2 \leq (1-\delta_1)^{-1}2s^2,$$

which shows that $C(n)$ is bounded, so that (iv) holds.

The proof that (iv) ⇒ (i) is more delicate. We skip the details. This was first proved in [28] using the Dudley-Fernique metric entropy condition together with a certain interpolation argument. Bourgain [3] gave a completely different proof. Both proofs show that (iv) implies that Λ is Sidon, as defined below, and then Sidon implies subgaussian (see Theorem 9.2). □

Remark 6.6. Note that in the proof that (i) ⇒ (ii) we actually showed that (iv) ⇒ (ii). Thus we gave a complete proof of the equivalence of (ii), (iii), (iii)' and (iv).

Remark 6.7. The proof that (iv) ⇒ (i) in [28] passes through the following

(v) Let $1 < p < 2$. There is a constant C such that for any f in the linear span of Λ we have

$$\|f\|_{\psi_{p'}} \leq C(\sum\nolimits_{n\in\Lambda} |\widehat{f}(n)|^p)^{1/p}.$$

We show in [28] that (iv) ⇒ (v) (this is an argument from the so-called real interpolation method). Then using special properties of the metric entropy integrals we show that (v) ⇒ Sidon, and hence (v) ⇒ (i) follows by Theorem 9.2.

7 Main open problem

We now come to the main open problem concerning subgaussian sets (or equivalently Sidon sets, that are defined in the next section) of characters on a compact Abelian group G.

Conjecture. *Any subgaussian set is a finite union of quasi-independent sets.*

The conjecture is supported by the case when $G = \mathbb{Z}(p)^{\mathbb{N}}$. Here $p > 1$ is a prime number and $Z(p) = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements. We have $\widehat{Z(p)} = Z(p)$. Indeed, any $n \in \mathbb{Z}/p\mathbb{Z}$ (represented, if we wish, by a number $n \in [0, p-1]$ modulo p) defines a character γ_n on $Z(p)$ by

$$\forall t \in Z(p) \quad \gamma_n(t) = e^{2\pi i t n/p}.$$

As before for $\mathbb{Z}$, the correspondence $n \leftrightarrow \gamma_n$ allows us to identify $\widehat{Z(p)}$ with $Z(p)$. One can also associate to γ_n the p-th root of unity $\gamma_n(1) = e^{2\pi i n/p}$.

Let $\mathbb{Z}(p)^{(\mathbb{N})} \subset \mathbb{Z}(p)^{\mathbb{N}}$ denote the set of sequences $n = (n_k) \in \mathbb{Z}(p)^{\mathbb{N}}$ with only finitely many nonzero terms. Let $n = (n_k) \in \mathbb{Z}(p)^{(\mathbb{N})}$. Then the function $\gamma_n : \mathbb{Z}(p)^{\mathbb{N}} \to \mathbb{T}$ defined by

$$\forall t = (t_k) \in Z(p)^{\mathbb{N}} \quad \gamma_n(t) = e^{2\pi i \sum t_k n_k/p},$$

is a character on $Z(p)^{\mathbb{N}}$, and all the characters are of this form. Thus again $n \leftrightarrow \gamma_n$ allows us to identify $\widehat{Z(p)^{\mathbb{N}}}$ with $Z(p)^{(\mathbb{N})}$.

The novel feature is that the group $\widehat{G} = \mathbb{Z}(p)^{(\mathbb{N})}$ is a vector space over the field $Z(p)$. Of course the scalar multiplication by $m \in \mathbb{Z}(p)$ is defined on $Z(p)^{(\mathbb{N})}$ in the natural way

$$\forall n = (n_k) \in Z(p)^{(\mathbb{N})} \quad m \cdot n = (mn_k).$$

For $G = Z(p)^{\mathbb{N}}$, a complete description of subgaussian sets of characters on G was given by Malliavin and Malliavin [25].

Theorem 7.1 ([25]). *Let $p > 1$ be a prime number. Let $G = Z(p)^{\mathbb{N}}$ and $\widehat{G} = \mathbb{Z}(p)^{(\mathbb{N})}$. Let $\Lambda \subset \widehat{G} \setminus \{0\}$. The following are equivalent:*

(i) Λ is subgaussian.

(ii) Λ is a finite union of linearly independent sets over the field $\mathbb{Z}/p\mathbb{Z}$.

(iii) Λ is a finite union of quasi-independent sets.

The miracle that produces this beautiful result is a deep (and difficult) combinatorial fact in linear algebra due to Horn [14] (published also by Rado but 10 years later), that says the following:

Theorem 7.2 ([14]). *Let Λ be a subset of a vector space over any field. Let $k > 0$ be an integer. Assume that any finite subset $A \subset \Lambda$ contains a (linearly) independent subset $B \subset A$ with $|B| \geq |A|/k$. Then (and only then) Λ can be decomposed as a union of k (linearly) independent subsets.*

Note that the assumption is clearly necessary for the conclusion to hold.

Proof of Theorem 7.1. Assume (i). We will apply the criterion of Theorem 7.2. Let $A \subset \Lambda$ be a finite subset. Let B be a maximal independent subset of A over the field $\mathbb{Z}/p\mathbb{Z}$. Then A must be included in the vector space V_B generated by B (indeed, if not we would find an element that we could add to B, and that would contradict the maximality of B). Clearly $\dim(V_B) = |B|$ and hence $|V_B| = p^{|B|}$. But now a fortiori V_B is finite group, and $sg(A) \leq sg(\Lambda)$, therefore by Corollary 5.5 we have for any $0 < \delta < 1$

$$\log|V_B| \geq |A|(1-\delta)^2/2sg(\Lambda)^2,$$

and hence if $\kappa = (1-\delta)^{-2}2sg(\Lambda)^2\log(p)$ and if k is the smallest integer such that $k \geq \kappa$

$$|B| \geq |A|/\kappa \geq |A|/k.$$

By Theorem 7.2 (ii) follows. Then (ii) ⇒ (iii) is obvious and (iii) ⇒ (i) follows from Remarks 5.9 and 5.2. □

Remark 7.3. In [4] Bourgain generalized (i) ⇔ (iii) in Theorem 7.1 to the case when $p = \prod p_k$ where $p_1, \cdots, p_n$ are distinct prime numbers. However, it seems that (i) ⇔ (iii) is still an open problem even for $p = 4$.

Remark 7.4. Let (γ_n) $(n \in \mathbb{N})$ be any sequence of characters on a compact Abelian group G. Thus each γ_n can be viewed as a random variable on (G, m_G) with values in $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. Assume first that there is no "torsion", i.e. that $\gamma_n^\xi \neq 1$ for any $\xi \neq 0$ $(\xi \in \mathbb{Z})$. Then (γ_n) are stochastically independent as random variables iff for any sequence $(\xi_n) \in \mathbb{Z}^{(\mathbb{N})}$ not identically $= 0$

$$\prod \gamma_n^{\xi_n} \not\equiv 1.$$

Equivalently, for any such (ξ_n)

$$\int \prod \gamma_n^{\xi_n} dm_G = 0.$$

Indeed, this condition holds iff for any n and any polynomials $Q_n(z, \bar{z})$ we have for any n

$$\int \prod\nolimits_1^n Q_k(\gamma_k) dm_G = \prod\nolimits_1^n \int Q_k(\gamma_k) dm_G.$$

To check this just replace polynomials by monomials.

Now assume ("torsion group") that there is a positive integer p_n such that $\gamma_n^{p_n} = 1$. We choose p_n minimal and we assume $p_n > 1$. Note that $\gamma_n^\xi = 1$ iff $\xi \in p_n\mathbb{Z}$. Then (γ_n) are stochastically independent as random variables iff for any sequence $(\xi_n) \in [0, p_n - 1]^{(\mathbb{N})}$ not identically $= 0$

$$\prod \gamma_n^{\xi_n} \not\equiv 1.$$

This shows that quasi-independence appears as a weaker form of stochastic independence. However, if $G = \{-1, 1\}^{\mathbb{N}}$ and if γ_n is the n-th coordinate on G then the two forms of independence coincide (here $p_n = 2$). This corresponds to the usual random choices of signs, as in Remark 1.13.

We note in passing that the classical Rademacher functions (r_n), which are defined on $([0,1], dt)$ by

$$\forall n \geq 0 \quad r_n(t) = \operatorname{sign}(\sin(2^n(2\pi t)))$$

form an i.i.d. sequence of uniformly distributed choices of signs. In sharp contrast, the sequence $(\exp i2^n(2\pi t))$ is only quasi-independent as a sequence of characters on $\mathbb{T}$.

Remark 7.5. Any Hadamard lacunary sequence $\Lambda = \{n(k)\}$ is a finite union of quasi-independent sets. Indeed, if (5.1) holds there must exist a number N such that

$$\forall n \quad |\Lambda \cap (2^n, 2^{n+1}]| \leq N.$$

This implies that Λ is the union of N sequences satisfying $|\Lambda \cap (2^n, 2^{n+1}]| \leq 1$ for all n. But then (by separating the n's into evens and odds) each such sequence is the union of two sequences such that $k(n) > \sum_{j<n} k(j)$ which by Remark 5.1 are quasi-independent.

Remark 7.6. There are quasi-independent sets in $\mathbb{N}$ that are not finite unions of Hadamard lacunary sets. Indeed, if Λ is such a finite union, then it is easy to see that there is a number K such that $|\Lambda \cap [2^n, 2^{n+1})| \leq K$ for any $n \geq 1$. The set

$$\{4^{n^2} + 2^j \mid n \geq 1, 1 \leq j \leq n\}$$

clearly violates that, but it is an easy exercise to check that it is quasi-independent.

Remark 7.7 ("Condition de maille"). By a variant of the argument in Theorem 5.3, one can show that any subgaussian set $\Lambda \subset \mathbb{Z}$ satisfies the following condition: there is a constant $K > 0$ such that for any $n, s > 0$ and any $k_1, \cdots, k_n \in \mathbb{Z}$

$$|\Lambda \cap \{k_1 m_1 + \cdots + k_n m_n \mid |m_1| + \cdots + |m_1| \leq 2^s\}| \leq Kns.$$

See [17, p. 71] for details. It seems to be still open whether this characterizes subgaussian sets.

By Theorem 6.5, the conjecture highlighted in this section is equivalent to the following purely combinatorial

Problem: *Let $\Lambda \subset \mathbb{Z}$. Assume that there is $\delta > 0$ such that any finite subset $A \subset \Lambda$ contains a quasi-independent $B \subset A$ with $|B| \geq \delta|A|$, does it follow that Λ is a finite union of quasi-independent sets?*

In 1983, I drew Paul Erdös's attention to this problem, raised in [29]. He became interested in the classes of sets that one could substitute to that of quasi-independent sets for which the problem would have an affirmative answer (see [8, 9]). He and his coauthors considered generalizations of the problem for graphs or hypergraphs, but the problem remains open.

8 Subgaussian bounded mean oscillation

The goal of this section is to show that the sequences of positive integers that can be written as a finite union of Hadamard-lacunary ones can be characterized as those that are subgaussian and remain subgaussian uniformly when restricted to an arbitrary subarc I equipped with its normalized Lebesgue measure m_I.

Here we prefer to think of $\mathbb{T}$ as the unit circle in $\mathbb{C}$. By a subarc we mean a connected subset of $\mathbb{T}$ with non empty interior. We denote by $\mathcal{I}$ the collection of all subarcs in $\mathbb{T}$. For any $I \in \mathcal{I}$, let $m_I = 1_I dt/|I|$ (normalized Lebesgue measure on I). For any $f \in L_1(\mathbb{T})$ we set

$$f_I = \int_I f dm_I$$

and

$$\|f\|_{*,1} = \left|\int f dm\right| + \sup_{I\in\mathcal{I}} \|f - f_I\|_{L_1(dm_I)} \in [0,\infty].$$

Note that for a complex-valued $f \in L_1(\mathbb{T})$ its real and imaginary parts satisfy obviously

$$\|\Re(f)\|_{*,1} \le \|f\|_{*,1} \quad \text{and} \quad \|\Im(f)\|_{*,1} \le \|f\|_{*,1}.$$

The space BMO($\mathbb{R}$) (resp. BMO($\mathbb{C}$)) of functions with bounded mean oscillation is defined as formed of all those *real-valued* (resp. *complex-valued*) $f \in L_1(\mathbb{T})$ such that $\|f\|_{*,1} < \infty$. Equipped with the norm $f \mapsto \|f\|_{*,1}$ it becomes a real (resp. complex) Banach space. This space is of crucial importance in the theory of H^p-spaces (see e.g. [11]).

The main point is that BMO($\mathbb{R}$) is the dual of H^1 (Fefferman's theorem). A priori, the space H^1 is a complex Banach space but for this duality theorem we view it as real space. Here we define H^1 as the closure in $L_1(\mathbb{T})$ of the linear span, denoted by $\mathcal{P}_+$, of the functions $\{e^{int} \mid n \ge 0\}$. We equip it with the norm induced by L_1, that we denote by $\|\ \|_{H^1}$. Fefferman's inequality establishes the duality, as follows:

$$\exists C_F > 0\ \forall f \in \text{BMO}(\mathbb{R}),\ \forall x \in \mathcal{P}_+$$
$$\left|\int f\Re(x)dm\right| \le C_F\|f\|_{*,1}\|x\|_{H^1}. \quad (8.1)$$

This shows that we can associate to each $f \in \text{BMO}(\mathbb{R})$ an $\mathbb{R}$-linear form $\xi_f : H^1 \to \mathbb{R}$, obtained by densely extending the functional $x \mapsto \xi_f(x) = \int f\Re(x)dm$ from $\mathcal{P}_+$ to the whole of H^1. It turns out that any $\mathbb{R}$-linear form $\xi : H^1 \to \mathbb{R}$ is of this form. Moreover, the norm $\|f\|_{*,1}$ is equivalent to the norm of $\xi_f : H^1 \to \mathbb{R}$. In other words, BMO($\mathbb{R}$) can be identified with the space of bounded $\mathbb{R}$-linear forms on H^1. We call the latter space the $\mathbb{R}$-linear dual of H^1, it is the dual of H^1 when we view the latter as a real Banach space. Thus the content of Fefferman's duality theorem is that BMO($\mathbb{R}$) is the $\mathbb{R}$-linear dual of H^1. We refer the reader to [11] for more on these topics.

In order to discuss other equivalent norms on the space BMO, for any $a > 0$ and $f \in L_1(\mathbb{T})$ we define

$$\|f\|_{*,\psi_a} = \left|\int f dm\right| + \sup_{I\in\mathcal{I}} \|f - f_I\|_{L_{\psi_a}(dm_I)} \in [0,\infty].$$

A famous theorem of John and Nirenberg asserts that $f \in BMO(\mathbb{C})$ iff $\|f\|_{*,\psi_1} < \infty$ and the norms $f \mapsto \|f\|_{*,1}$ and $f \mapsto \|f\|_{*,\psi_1}$ are equivalent. (A fortiori, the same holds for $f \mapsto \|f\|_{*,\psi_a}$ for any $0 < a \le 1$.) This particular fact is even valid for Banach space valued functions. We refer to our recent book [32] for more information on Banach space valued H^p-spaces.

It is well known that the norms $f \mapsto \|f\|_{*,1}$ or $f \mapsto \|f\|_{*,\psi_1}$ are *not* equivalent to the norm $f \mapsto \|f\|_{*,\psi_a}$ when $a > 1$. Nevertheless, the norm $f \mapsto \|f\|_{*,\psi_2}$ is equivalent to the usual BMO norm $f \mapsto \|f\|_{*,1}$ when restricted to f in the linear span of $\{\exp(in_k t)\}$ if the sequence $\{n_k\}$ is a finite union of Hadamard lacunary sequences. This was proved in [20]. (Closely related results appear in [6]). More precisely, it turns out that this characterizes such sequences.

Theorem 8.1. *Let $n_0 < n_1 < \cdots < n_k < \cdots$ be integers. Let $\Lambda = \{n_k\}$. The following are equivalent:*

(i) The set $\Lambda = \{n_k\}$ is a finite union of Hadamard lacunary sets.

(ii) There is a constant C such that for any $x \in \ell_2$ we have

$$\|\textstyle\sum_k x_k e^{in_k t}\|_{*,\psi_2} \le C(\sum |x_k|^2)^{1/2}.$$

(iii) There is a constant C such that for any $x \in \ell_2$ we have

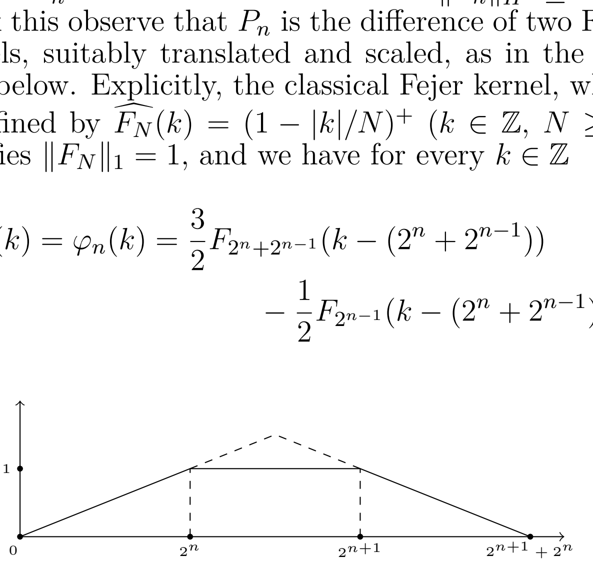
$$\|\textstyle\sum_k x_k e^{in_k t}\|_{*,1} \le C(\sum |x_k|^2)^{1/2}.$$

Proof. The key fact here is that (i) ⇒ (ii). It suffices obviously to prove (ii) assuming that the sequence $\{n_k\}$ is itself lacunary. This is proved in detail in [20] to which we refer the reader.

(ii) ⇒ (iii) is obvious.

Assume (iii). We claim that there is a constant N such that for any $n \ge 1$ $|\Lambda \cap [2^n, 2^{n+1}]| \le N$. From this claim, as already mentioned it is easy to deduce (i) (see Remark 7.5). To prove the claim, fix $n \ge 1$ and let $\varphi_n : \mathbb{N} \to \mathbb{R}$ be the function defined by the graph in the picture below. More explicitly, $\varphi_n(k) = 1$ $\forall k \in [2^n, 2^{n+1}]$, $\varphi_n(k) = 0$ $\forall k \notin (0, 2^{n+1} + 2^n)$ and φ_n passes affinely from 0 to 1 (resp. 1 to 0) on the interval $[0, 2^n]$ (resp. $[2^{n+1}, 2^{n+1} + 2^n]$). We then consider the trigonometric polynomial $P_n \in \mathcal{P}_+$ defined on $\mathbb{T}$ by $P_n(t) = \sum_{k\ge0} \varphi_n(k)e^{ikt}$, so that φ_n is the Fourier transform of P_n. It is a well known fact that $\|P_n\|_{H^1} \le 2$. To check this observe that P_n is the difference of two Fejer kernels, suitably translated and scaled, as in the picture below. Explicitly, the classical Fejer kernel, which is defined by $\widehat{F_N}(k) = (1 - |k|/N)^+$ $(k \in \mathbb{Z},\ N \ge 1)$ satisfies $\|F_N\|_1 = 1$, and we have for every $k \in \mathbb{Z}$

$$\widehat{P_n}(k) = \varphi_n(k) = \frac{3}{2}F_{2^n+2^{n-1}}(k - (2^n + 2^{n-1}))$$
$$- \frac{1}{2}F_{2^{n-1}}(k - (2^n + 2^{n-1})).$$



Let $f = \sum_k x_k e^{in_k t}$. By (8.1) we have

$$\begin{aligned}|\sum_k \varphi_n(n_k)x_k/2| &= \int f(t)\Re(P_n(t))dm| \\ &\leq |\int \Re(f(t))\Re(P_n(t))dm| + \\ &\qquad\qquad |\int \Im(f(t))\Re(P_n(t))dm| \\ &\leq C_F\|\Re(f)\|_{*,1}\|P_n\|_{H^1} + C_F\|\Im(f)\|_{*,1}\|P_n\|_{H^1} \\ &\leq 2C_F\|f\|_{*,1}\|P_n\|_{H^1} \\ &\leq 4C_F C(\sum |x_k|^2)^{1/2}.\end{aligned}$$

Taking the supremum of the left hand side over all (x_k) such that $(\sum |x_k|^2)^{1/2} \leq 1$ we obtain

$$(\sum_k \varphi_n(n_k)^2)^{1/2}/2 \leq 4C_F C.$$

A fortiori, recalling $\varphi_n(k) = 1\ \forall k \in [2^n, 2^{n+1}]$, this implies

$$|\Lambda \cap [2^n, 2^{n+1}]| \leq (8C_F C)^2.$$

This proves the claim and concludes the proof. □

9 Sidon sets

The notion of Sidon set, or more generally of “thin set", has a long history. See the classical books [15, 23, 13]. For a more recent account see [12]. There are many connections between Sidon sets and random Fourier series. See [24] for more in this direction. In general Kahane's books [16, 17] are a wonderful introduction to the use of random functions in harmonic analysis. The many connections with Banach space theory are presented in [22].

Definition. Let $\Lambda = \{\varphi_n \mid n \geq 1\}$ be a bounded sequence in $L_\infty(T, m)$ ((T, m) being a probability space). We say that Λ is Sidon if there is a constant C such that for any finitely supported scalar sequence (a_n) we have

$$\sum |a_n| \leq C\|\sum a_n\varphi_n\|_\infty.$$

Note that if $C' = \sup_{n\geq 1}\|\varphi_n\|_\infty$ we have obviously

$$\|\sum a_n\varphi_n\|_\infty \leq C'\sum |a_n|.$$

Let Λ be a set of continuous characters on a compact Abelian group G. We may view Λ as a subset of $L_\infty(G, m_G)$. For instance when $G = \mathbb{T}$ we may identify Λ with a subset of $\mathbb{Z}$, and we view

$$\{\varphi_n \mid n \geq 1\} = \{e^{int} \mid n \in \Lambda\}$$

The study of Sidon sets, or more generally of ‘thin" sets, was a very active subject in harmonic analysis in the 1960's and 1970's. A puzzling problem that played an important role there early on was the union problem: whether (in the case of sets of characters) the union of two Sidon sets is a Sidon set. The difficulty is that if Λ_1 and Λ_2 are disjoint sets in $\widehat{G}$ there is a priori no inequality of the form

$$\|\sum_{n\in\Lambda_1} a_n\varphi_n\|_\infty \leq C\|\sum_{n\in\Lambda_1\cup\Lambda_2} a_n\varphi_n\|_\infty.$$

The union problem was eventually solved positively by Sam Drury in 1970 using a very beautiful argument involving convolution in measure algebras (see [23]).

Rider [34] refined Drury's trick and connected Sidon sets with random Fourier series. To explain this we need one more definition. Recall that (ε_n) is an i.i.d. sequence of choices of signs on a probability space $(\Omega, \mathbb{P})$, i.e. (ε_n) are independent and $\mathbb{P}\{\varepsilon_n = \pm 1\} = 1/2$.

Definition. Let $\Lambda = \{\varphi_n \mid n \geq 1\}$ be a bounded sequence in $L_\infty(T, m)$ ((T, m) being a probability space). We say that Λ is randomly Sidon if there is a constant C such that for any finitely supported scalar sequence (a_n) we have

$$\sum |a_n| \leq C\mathbb{E}\|\sum \varepsilon_n a_n\varphi_n\|_\infty.$$

Theorem 9.1 (Rider [34]). *Let $\Lambda \subset \mathbb{Z}$ or more generally $\Lambda \subset \widehat{G}$ ($\widehat{G}$ any discrete Abelian group). If Λ is randomly Sidon then it is Sidon (and the converse is trivial).*

Rider's proof of this theorem can be interpreted as a refinement of Drury's, and indeed, Rider's Theorem implies that the union of two Sidon sets is a Sidon set, because it is easy to check that the union of two randomly Sidon sets is randomly Sidon. Indeed, now if Λ_1 and Λ_2 are disjoint sets in $\widehat{G}$ we do have

$$\mathbb{E}\|\sum_{n\in\Lambda_1} \varepsilon_n a_n\varphi_n\|_\infty \leq \mathbb{E}\|\sum_{n\in\Lambda_1\cup\Lambda_2} \varepsilon_n a_n\varphi_n\|_\infty.$$

The connection with subgaussian sequences originates in the following

Theorem 9.2 ([35, 27]). *Let $\Lambda \subset \mathbb{Z}\setminus\{0\}$ or more generally $\Lambda \subset \widehat{G}\setminus\{0\}$ ($\widehat{G}$ any discrete Abelian group). Then Λ is Sidon if and only if it is subgaussian.*

Rudin proved that Sidon implies subgaussian and asked whether the converse was true. We proved this in [27], using Gaussian random Fourier series. Bourgain [3] gave a more direct proof avoiding random Fourier series. In any case, Drury's ideas are still somewhere in the background, and this is not surprising: indeed, it is obvious (recall (1.10)) that the union of two subgaussian sequences is a subgaussian sequence.

Proof of Theorem 9.2. Assume $\Lambda \subset \widehat{G}$ Sidon. Let $M(G)$ be the space of (complex) measures on G equi-pped with the total variation norm $\|\mu\|_{M(G)} = |\mu|(G)$. Recall the identification $M(G) = C(G)^*$. Let us enumerate $\Lambda = \{\gamma_n \mid n \in \mathbb{N}\}$. For any $z = (z_n) \in \mathbb{T}^{\mathbb{N}}$ and any

$f \in \text{span}(\Lambda)$ we have

$$|\sum z_n \int \overline{\gamma_n} f dm_G| \le \sum_{\gamma\in\Lambda} |\widehat{f}(\gamma)| \le C\|f\|_{C(G)}.$$

By Hahn-Banach there is a $\nu_z \in M(G)$ with $\|\nu\|_{M(G)} \le C$ such that $\nu_z(f) = \sum z_n \int \overline{\gamma_n} f dm_G$ or equivalently $\nu_z(\gamma_n) = z_n$ for all n. Let μ_z be the symmetric of ν_z defined by $\mu_z(f) = \int f(-t)\nu_z(dt)$. Then $\widehat{\mu_z}(\gamma_n) = z_n$ for all n. Let $f \in \text{span}(\Lambda)$, say $f = \sum a_n\gamma_n$. Then $\mu_z * f = \sum a_n z_n \gamma_n$ and

$$\|\mu_z * f\|_p \le C\|\mu_z\|_{M(G)} \le C\|f\|_p.$$

But we may apply this last inequality also to $f = \sum a_n \overline{z_n}\gamma_n$. This gives us

$$\forall z \in \mathbb{T}^{\mathbb{N}} \quad \|\sum a_n\gamma_n\|_p \le C\|\sum z_n a_n \gamma_n\|_p.$$

Integrating the p-th power over z we find

$$\|\sum a_n\gamma_n\|_p \le C\left(\int |\sum z_n a_n \gamma_n(t)|^p dm_G(t) dm_{\mathbb{T}^{\mathbb{N}}}(z)\right)^{1/p}$$

and by the translation invariance of $m_{\mathbb{T}^{\mathbb{N}}}$ this last term is the same as $C(\int |\sum z_n a_n|^p dm_{\mathbb{T}^{\mathbb{N}}}(z))^{1/p}$. Therefore we obtain

$$\|\sum a_n\gamma_n\|_p \le C(\int |\sum z_n a_n|^p dm_{\mathbb{T}^{\mathbb{N}}}(z))^{1/p}.$$

But since we know (see Remark 1.13) that $sg(z_n) \le 1$, by Lemma 3.2 we obtain

$$\|\sum a_n\gamma_n\|_p \le C\beta\sqrt{p}(\sum |a_n|^2)^{1/2}$$

where β is a numerical constant. By Lemma 3.2 again, $\Lambda = (\gamma_n)$ is subgaussian.
That subgaussian implies Sidon will be fully proved in a more general framework in the next section (see Remark 10.3). □

10 Subgaussian bounded orthonormal systems

Recently Bourgain and Lewko [5] tried to understand what remains true for general bounded orthonormal systems of the equivalences described in §9, namely the equivalence between Sidon, randomly Sidon and subgaussian.

Obviously Sidon ⇒ randomly Sidon remains true. However, it is easy to see that Sidon $\not\Rightarrow$ subgaussian for general orthonormal systems bounded in L_∞. Indeed, if (φ_n) is Sidon say on $([0,1], dt)$ then any system on $([0,2], dt/2)$ that coincides with (φ_n) on $[0,1]$ is still Sidon, but if its restriction to $[1,2]$ is not subgaussian, the resulting system on $([0,2], dt/2)$ cannot be subgaussian. For the converse implication, it turns out to be more delicate to produce a counterexample but Bourgain and Lewko [5] managed to do that. Nevertheless, they proved that subgaussian implies $\otimes^5$-Sidon in the following sense:

Definition 10.1. Let $k \ge 1$. We say that (φ_n) is $\otimes^k$-Sidon with constant C if the system $\{\varphi_n(t_1)\cdots\varphi_n(t_k)\}$ (or equivalently $\{\varphi_n^{\otimes k}\}$) is Sidon with constant C in $L_\infty(T^k, m^{\otimes k})$.

In [5] they asked whether 5 could be replaced by 2, and in [27] we showed that indeed it is so:

Theorem 10.2. *Any subgaussian system bounded in $L_\infty(T,m)$ and orthonormal in $L_2(T,m)$ is $\otimes^2$-Sidon.*

Remark 10.3. The preceding result (as well as the previous one obtaining $\otimes^5$-Sidon) implies the result stated in Theorem 9.2 that for subsets of $\widehat{G}$ ($\widehat{G}$ discrete Abelian group) subgaussian implies Sidon. Indeed, if the functions φ_n are characters then the identity $\varphi_n(t_1\cdots t_k) = \varphi_n(t_1)\cdots\varphi_n(t_k)$ shows that for characters $\otimes^k$-Sidon ⇒ Sidon.

The key to the proof of Theorem 10.2 is the next statement, for which we need to recall the definitions of the projective and injective tensor norms, respectively $\|\ \|_\wedge$ and $\|\ \|_\vee$ on the algebraic tensor product $L_1(m_1)\otimes L_1(m_2)$ (here $(T_1,m_1),(T_2,m_2)$ are arbitrary measure spaces). Let $T \in L_1(m_1)\otimes L_1(m_2)$ say $T = \sum x_j \otimes y_j$ we set

$$\|T\|_\wedge = \int |\sum x_j(t_1)y_j(t_2)| dm_1(t_1)dm_2(t_2)$$

$$\|T\|_\vee = \sup\{|\sum\langle x_j,\psi_1\rangle\langle y_j,\psi_2\rangle| \mid \|\psi_1\|_\infty \le 1, \|\psi_2\|_\infty\}.$$

Note that the completion of $L_1(m_1)\otimes L_1(m_2)$ with respect to $\|\ \|_\wedge$ can be identified isometrically to $L_1(m_1\times m_2)$.

Theorem 10.4. *Let (T,m) be a probability space. Let (g_n) be an i.i.d. sequence of normalized $\mathbb{R}$-Gaussian random variables. For any $0<\delta<1$ there is $w(\delta)>0$ for which the following property holds. Let*

$$\{\varphi_n \mid 1 \le n \le N\} \subset L_1(m)$$

be any system that is C-dominated by $\{g_n \mid 1 \le n \le N\}$. Then, for any $(z_n) \in \mathbb{C}^N$ with $|z_n| \le 1$, there is a decomposition in $L_1(m)\otimes L_1(m)$ of the form

$$\sum\nolimits_1^N z_n\varphi_n \otimes \varphi_n = t + r \tag{10.1}$$

satisfying

$$\|t\|_\wedge \le Cw(\delta) \quad \textit{and} \quad \|r\|_\vee \le C\delta. \tag{10.2}$$

Proof. It clearly suffices to prove this in the case $\varphi_n = g_n$ and $C = 1$ (indeed, the classical properties of tensor products allow us to pass from g_n to φ_n). Moreover, treating separately $\sum_1^N \Re(z_n)\varphi_n\otimes\varphi_n$ and $\sum_1^N \Im(z_n)\varphi_n\otimes\varphi_n$, we may reduce to the case when the z_n's are in $[-1,1]$. But then, by Lemma 2.1 there is an operator $\Theta_z : L_1(\mathbb{P}) \to L_1(\mathbb{P})$ with norm 1 such that $T_z(g_n) = z_n g_n$. Using this, we can reduce to the case when $z_n = 1$ for all n. We will show that Theorem 10.4 can be easily derived from the following

Claim: for any $0 < \delta < 1$ there is $\Phi \in L_1(\mathbb{P} \times \mathbb{P})$ with $\|\Phi\|_{L_1(\mathbb{P}\times\mathbb{P})} = 1$ such that

$$\Phi = 1 \otimes 1 + \delta \sum\nolimits_1^N g_n \otimes g_n + R$$

where R viewed as an operator on $L_2(\mathbb{P})$ has norm $\leq \delta^2$. This claim is immediate from the discussion in §2. We just take for Φ the Mehler kernel and note that P_1 can be identified with $\sum_1^N g_n \otimes g_n$ and we have

$$\| \sum\nolimits_{d \geq 2} \delta^d P_d : \ L_2(\mathbb{P}) \to L_2(\mathbb{P})\| \leq \delta^2.$$

From the claim we deduce

$$\sum\nolimits_1^N g_n \otimes g_n = t' + r'$$

with $t' = (\Phi - 1 \otimes 1)/\delta$ and $r' = -R/\delta$. Then we have

$$\|t'\|_{L_1(\mathbb{P}\times\mathbb{P})} \leq 2/\delta$$

and

$$\|r'\|_{\vee} \leq \|r : \ L_2(\mathbb{P}) \to L_2(\mathbb{P})\| \leq \delta.$$

The only problem is that t (and hence also r) are in the space $L_1(\mathbb{P} \times \mathbb{P})$ and we want them to be in $L_1(\mathbb{P}) \otimes L_1(\mathbb{P})$. In other words we want the associated operators to be of finite rank. This can be fixed like this: it is a well known property of L_1-spaces that for any $\varepsilon > 0$ and any finite dimensional subspace $E \subset L_1$ there is a finite rank operator $v : \ L_1 \to L_1$ with $\|v\| < 1 + \varepsilon$ that is the identity on E. We apply this to $E = \text{span}[g_n \mid 1 \leq n \leq N]$ with (say) $\varepsilon = 1$, and then we set $t = (v \otimes Id)(t')$ and $r = (v \otimes Id)(r')$. This gives us finite rank tensors satisfying the desired conclusion with $\|t\|_\wedge \leq 4/\delta$ and $\|r\|_\vee \leq 2\delta$. Since we may trivially replace δ by $\delta/2$, the proof is complete. □

Proof of Theorem 10.2. Let $C' = \sup_n \|\varphi_n\|_\infty$. Note that (φ_n) is subgaussian iff $(\overline{\varphi_n})$ also is, with the same constant. By Proposition 4, any subgaussian system is C-dominated by (g_n) for some C. Let $z_n \in \mathbb{T}$ be such that $|a_n| = \varepsilon_n a_n$. Let $\sum z_n \overline{\varphi_n} \otimes \overline{\varphi_n} = t + r$ as in (10.2). Let $f(t_1, t_2) = \sum a_n \varphi_n(t_1)\varphi_n(t_2)$. We have

$$\langle t + r, f\rangle = \int (\sum z_n \overline{\varphi_n} \otimes \overline{\varphi_n}) f = \sum z_n a_n = \sum |a_n|.$$

Therefore

$$\begin{aligned} \sum |a_n| &\leq |\langle t, f\rangle| + |\langle r, f\rangle| \\ &\leq Cw(\delta)\|f\|_\infty + \sum |a_n| |\langle r, \overline{\varphi_n} \otimes \overline{\varphi_n}\rangle| \\ &\leq Cw(\delta)\|f\|_\infty + C\delta C'^2 \sum |a_n|. \end{aligned}$$

Choosing δ such that $\delta C C'^2 = 1/2$ we conclude that $(\varphi_n \otimes \varphi_n)$ is Sidon with constant $\leq 2Cw(\delta)$. □

Remark 10.5. It is proved in [33] that, in the situation of Theorem 10.2 (φ_n) is randomly Sidon iff it is $\otimes^k$-Sidon for some (or equivalently for all) $k \geq 4$. This extends Rider's Theorem 9.1 to bounded orthonormal systems. Here, the cases $k = 2$ and $k = 3$ remain open.

Remark 10.6. Let (φ_n) be uniformly bounded and orthonormal. The same interpolation argument alluded to in Remark 6.7 shows that if (φ_n) is subgaussian (or if it merely satisfies the analogue of (iv) in Theorem 6.5) then for any $1 < p < 2$ there is a constant C_p such that for any $f = \sum a_n \varphi_n$ in its linear span we have

$$\|f\|_{\psi_{p'}} \leq C_p (\sum |a_n|^p)^{1/p}. \tag{10.3}$$

Actually, one can even prove $\|f\|_{\psi_{p'}} \leq C_p \|(a_n)\|_{p,\infty}$, where $\|(a_n)\|_{p,\infty} = \sup_{n\geq 1} n^{1/p} a_n^*$ (here

$$a_1^* \geq a_2^* \geq \cdots \geq a_n^* \geq \cdots$$

is the non-increasing rearrangement of $(|a_n|)$.

Problem: Does (10.3) imply that (φ_n) is $\otimes^k$-Sidon for some $k > 1$?

References

[1] S. Artstein-Avidan, A. Giannopoulos and V. Milman, Asymptotic geometric analysis. Part I. Mathematical Surveys and Monographs, 202. American Mathematical Society, Providence, RI, 2015.

[2] K. Azuma, Weighted sums of certain dependent random variables, *Tôhoku Math. J.* **19** (1967) 357–367.

[3] J. Bourgain, Sidon sets and Riesz products. Ann. Inst. Fourier (Grenoble) 35 (1985), 137–148.

[4] J. Bourgain, Propriétés de décomposition pour les ensembles de Sidon. Bull. Soc. Math. France 111 (1983), 421–428.

[5] J. Bourgain and M. Lewko, Sidonicity and variants of Kaczmarz's problem, preprint, arxiv, April 2015.

[6] S.-Y. A. Chang, J. M. Wilson and T. H. Wolff, Some weighted norm inequalities concerning the Schrd̈inger operators. Comment. Math. Helv. 60 (1985), 217–246.

[7] B.S.Cirel'son, I.A.Ibragimov and V.N.Sudakov, Norms of Gaussian sample functions, Proceedings of the Third Japan-USSR Symposium on Probability Theory (Tashkent, 1975), pp. 20–41. Lecture Notes in Math., Vol. 550, Springer, Berlin, 1976.

[8] P. Erdös, J. Nesetril and V. Rödl, On Pisier type problems and results (combinatorial applications to number theory). Mathematics of Ramsey theory, 214–231, Algorithms Combin., 5, Springer, Berlin, 1990.

[9] P. Erdös, J. Nesetril and V. Rödl, A remark on Pisier type theorems, Congressus Numerantium 113 (1996) 101–109.

[10] X. Fernique, Régularité des trajectoires des fonctions aléatoires gaussiennes, *Springer Lecture Notes in Math.*, **480** (1975), 1–96.

[11] J. Garnett, *Bounded analytic functions*, Academic Press, New-York, 1981.

[12] C. Graham and K. Hare, *Interpolation and Sidon sets for compact groups*. Springer, New York, 2013. xviii+249 pp.

[13] C. Graham and O.C. Mc Gehee, *Essays in commutative harmonic analysis*. Springer-Verlag, New York-Berlin, 1979.

[14] A. Horn, A characterization of unions of linearly independent sets. J. London Math. Soc. 30, (1955), 494–496.

[15] E. Hewitt and K. Ross, *Abstract harmonic analysis, Volume II, Structure and Analysis for Compact Groups, Analysis on Locally Compact Abelian Groups*, Springer, Heidelberg, 1970.

[16] J. P. Kahane, *Séries de Fourier absolument convergentes* Springer, 1970.

[17] J. P. Kahane, *Some random series of functions. Second edition* , Cambridge University Press, 1985.

[18] M. Ledoux, *The concentration of measure phenomenon*, Mathematical Surveys and Monographs, 89. American Mathematical Society, Providence, RI, 2001.

[19] M. Ledoux and M. Talagrand, *Probability in Banach Spaces. Isoperimetry and Processes*, Springer-Verlag, Berlin, 1991.

[20] H. Lelièvre, Espaces BMO, inégalités de Paley et multiplicateurs idempotents. Studia Math. 123 (1997), 249–274.

[21] M. Lévy, Prolongement d'un opérateur d'un sous-espace de $L^1(\mu)$ dans $L_1(\nu)$. Séminaire d'Analyse Fonctionnelle 1979–1980, Exp. No. 5, École Polytech., Palaiseau, 1980.

[22] D. Li and H. Queffélec, Introduction à l'étude des espaces de Banach. Société Mathématique de France, Paris, 2004.

[23] J. López and K.A. Ross, *Sidon sets.* Lecture Notes in Pure and Applied Mathematics, Vol. 13. Marcel Dekker, Inc., New York, 1975.

[24] M.B. Marcus and G. Pisier, *Random Fourier series with Applications to Harmonic Analysis.* Annals of Math. Studies n°101, Princeton Univ. Press, 1981.

[25] M.P. Malliavin and P. Malliavin, Caractérisation arithmétique d'une classe d'ensembles de Helson, C. R. Acad. Sci. Paris Sér. A-B 264 (1967) A192–A193.

[26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

[27] G. Pisier, Ensembles de Sidon et processus gaussiens. C.R. Acad. Sc. Paris, t. A 286 (1978) 671–674.

[28] G. Pisier, De nouvelles caractérisations des ensembles de Sidon. Advances in Maths. Supplementary studies, vol 7B (1981) 685–726.

[29] G. Pisier, Arithmetic characterizations of Sidon sets. Bull. A.M.S. (1983) 8, 87–90.

[30] G. Pisier, Probabilistic methods in the geometry of Banach spaces, Probability and analysis (Varenna, 1985), 167–241, *Lecture Notes in Math.* 1206, Springer-Verlag, Berlin, 1986.

[31] G. Pisier, Complex interpolation and regular operators between Banach lattices. Archiv der Mat. (Basel) 62 (1994) 261–269.

[32] G. Pisier, *Martingales in Banach spaces.* Cambridge Univ. Press, 2016.

[33] G. Pisier, On uniformly bounded orthonormal Sidon systems. Preprint, arxiv 2016.

[34] D. Rider, Randomly continuous functions and Sidon sets. Duke Math. J. 42 (1975) 752–764.

[35] W. Rudin, Trigonometric series with gaps. J. Math. and Mech. 9 (1960) 203–227.

[36] V. N. Sudakov and B. S. Tsirelson, Extremal properties of half-spaces for spherically invariant measures. J. Soviet. Math. 9 (1978), 9–18 ; translated from Zap. Nauch. Sem. L.O.M.I. 41, 14–24 (1974).

[37] M. Talagrand, Regularity of Gaussian processes. Acta Math., 159 (1987), 99–149.

[38] M. Talagrand, Majorizing measures: the generic chaining, Ann. Probab. 24 (1996), 1049–1103.

[39] M. Talagrand, *Upper and Lower Bounds for Stochastic Processes*, Springer, Berlin, 2014.

Gilles Pisier: Texas A&M University and UPMC-Paris VI