Performance Estimates of the Pseudo-Random Method for Radar Detection

Alexander Fish and Shamgar Gurevich

***Abstract*—A performance of the pseudo-random method for the radar detection is analyzed. The radar sends a pseudo-random sequence of length N, and receives echo from r targets. We assume the natural assumptions of uniformity on the channel and of the square root cancellation on the noise. Then for $r \leq N^{1-\delta}$, where $\delta > 0$, the following holds: (i) the probability of detection goes to one, and (ii) the expected number of false targets goes to zero, as N goes to infinity.**

I. Introduction

A RADAR is designed to estimate the location and velocity of objects in the surrounding space. The radar performs sensing by analyzing correlations between sent and received (analog) signals. In this note we describe the digital radar, i.e. we assume that the radar sends and receives finite sequences. The reduction to digital setting can be carried out in practice, see for example [1], and [5].

Throughout this note we denote by $\mathbb{Z}_N$ the set of integers $\{0, 1, ..., N-1\}$ equipped with addition and multiplication modulo N. We denote by $\mathcal{H} = \mathbb{C}(\mathbb{Z}_N)$ the vector space of complex valued functions on $\mathbb{Z}_N$ equipped with the standard inner product $\langle \cdot, \cdot \rangle$, and refer to it as the *Hilbert space of sequences*. We use the notation $S_{\mathbb{C}}^{r-1}$ to denote the unit complex sphere in $\mathbb{C}^r$:

$$S_{\mathbb{C}}^{r-1} = \{(z_1, \dots, z_r) \in \mathbb{C}^r \mid \sum_{k=1}^{r} |z_k|^2 = 1\}.$$

A. Model of Digital Radar

We describe the discrete radar model which was derived in [1]. We assume that a radar sends a sequence $S \in \mathcal{H}$ and receives as an echo a sequence $R \in \mathcal{H}$. The relationship between S, and R is given by the following equation:

$$R[n] = H(S)[n] + \mathcal{W}[n], \ n \in \mathbb{Z}_N, \tag{I-A.1}$$

where H, called the *channel operator*, is defined by[1]

$$H(S)[n] = \sum_{k=1}^{r} \alpha_k e(\omega_k n) S[n - \tau_k], \ n \in \mathbb{Z}_N, \tag{I-A.2}$$

with α_k's the complex-valued attenuation coefficients associated with target k, $\|\vec{\alpha}\|^2 = \sum_k |\alpha_k|^2 = 1$, $\tau_k \in \mathbb{Z}_N$ the time shift associated with target k, $\omega_k \in \mathbb{Z}_N$ the frequency shift associated with target k, and $\mathcal{W}$ denotes a *random* noise. The parameter r will be called the *sparsity* of the channel. The time-frequency shifts (τ_k, ω_k) are related to the location and velocity of target k. We denote the plane $\mathbb{Z}_N \times \mathbb{Z}_N$ of all time-frequency shifts by V. We denote by P the probability measure on the sample space generated by the random noise and attenuation coefficients.

Remark I-A.1: Let us elaborate on the constraint $\|\vec{\alpha}\| = 1$. In reality $\|\vec{\alpha}\| \leq 1$. However, we can rescale the received sequence R to make $\|\vec{\alpha}\| = 1$. The rescaling will not change the quality of the detection, as evident from Section II-C.

We make the following assumption on the distribution of $\mathcal{W}$:

Assumption (**Square root cancellation**): For every $\varepsilon > 0$, there exists $c > 0$, such that for any N^2 vectors $u_1, \dots, u_{N^2} \in S_{\mathbb{C}}^{N-1}$ we have

$$P\left(|\langle \mathcal{W}, u_j \rangle| \leq N^{-\frac{1}{2}+\varepsilon}, \ j = 1, 2, \dots, N^2\right) \geq 1 - e^{-cN}.$$

Note that an additive white gaussian noise (AWGN) of a constant, i.e., independent of N, signal-to-noise ratio (SNR) satisfies this assumption.

In addition, we make the following natural assumption on the distribution of the attenuation coefficients $(\alpha_1, \dots, \alpha_r)$ of the channel operator:

Assumption (**Uniformity**): For any measurable subset $E \in S_{\mathbb{C}}^{r-1}$ we have

$$P\left((\alpha_1, \dots, \alpha_r) \in E\right) = \frac{Area(E)}{Area(S_{\mathbb{C}}^{r-1})},$$

where $Area$ denotes the unique up to scaling non-negative Borel measure on $S_{\mathbb{C}}^{r-1}$ which is invariant under all rotations of $\mathbb{C}^r$, i.e., elements in $SO_r(\mathbb{C})$.

The last natural assumption that we make is the independence of the noise and of the vector of attenuation coefficients of the channel operator:

Assumption (**Independence**): The random sequences $\mathcal{W} \in \mathcal{H}$ and $\vec{\alpha} = (\alpha_1, \dots, \alpha_r) \in S_{\mathbb{C}}^{r-1}$ are independent.

B. Objectives of the Paper

The main task of the digital radar system is to extract the channel parameters (τ_k, ω_k), $k = 1, ..., r$, using S and R satisfying (I-A.1). One of the most popular methods for channel estimation is the pseudo-random (PR) method. In this note we describe the PR method and analyze its performance.

This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) award number N66001-13-1-4052. This work was also supported in part by NSF Grant DMS-1101660 - "The Heisenberg–Weil Symmetries, their Geometrization and Applications".

A. Fish is with School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia. Email: alexander.fish@sydney.edu.au.

S. Gurevich is with the Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA. Email: shamgar@math.wisc.edu.

[1]We denote $e(t) = \exp(2\pi i t/N)$.

II. Ambiguity Function and Pseudo-Random Method

A classical method to estimate the channel parameters in (I-A.1) is the *pseudo-random method* [2], [3], [4], [5], [6]. It uses two ingredients - the ambiguity function, and a pseudo-random sequence.

A. *Ambiguity Function*

In order to reduce the noise component in (I-A.1), it is common to use the ambiguity function that we are going to describe now. We consider the time-frequency shift operators $\pi(\tau,\omega)$, $\tau,\omega \in \mathbb{Z}_N$, which act on $f \in \mathcal{H}$ by

$$[\pi(\tau,\omega)f]\,[n] = e(\omega n)\cdot f[n-\tau],\ \ n \in \mathbb{Z}_N \tag{II-A.1}$$

The *ambiguity function* of two sequences $f, g \in \mathcal{H}$ is defined as the $N \times N$ matrix

$$\mathcal{A}(f,g)[\tau,\omega] = \langle \pi(\tau,\omega)f, g\rangle\,, \quad \tau,\omega \in \mathbb{Z}_N. \tag{II-A.2}$$

*Remark II-A.1 (**Fast Computation of Ambiguity Function**):* The restriction of the ambiguity function to a line in the time-frequency plane, can be computed in $O(N\log N)$ arithmetic operations using fast Fourier transform. For more details, including explicit formulas—see Section V of [1]. Overall, we can compute the entire ambiguity function in $O(N^2\log N)$ operations.

B. *Pseudo-Random Sequences*

We say that a norm-one sequence $\varphi \in \mathcal{H}$ is *B-pseudo-random*, $B \in \mathbb{R}$—see Figure 1 for illustration—if for every $(\tau,\omega) \neq (0,0)$ we have

$$|\mathcal{A}(\varphi,\varphi)[\tau,\omega]| \leq B/\sqrt{N}. \tag{II-B.1}$$

There are several constructions of families of pseudo-random (PR) sequences in the literature—see [2], [3] and references therein.

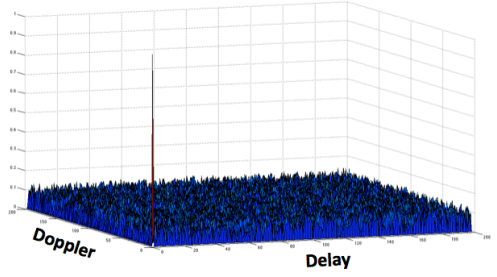

Fig. 1. Profile of $\mathcal{A}(\varphi,\varphi)$ for φ pseudo-random sequence.

C. *Pseudo-Random (PR) Method*

Consider a pseudo-random sequence φ, and assume for simplicity that $B = 1$ in (II-B.1). Then we have

$$\mathcal{A}(\varphi, H(\varphi))[\tau,\omega] \tag{II-C.1}$$
$$= \begin{cases} \widetilde{\alpha}_k + \sum\limits_{j\neq k} \widetilde{\alpha}_j/\sqrt{N}, & \text{if } (\tau,\omega) = (\tau_k,\omega_k)\,,\ 1 \leq k \leq r; \\ \sum\limits_j \widehat{\alpha}_j/\sqrt{N}, & \text{otherwise,} \end{cases}$$

where $\widetilde{\alpha}_j$, $\widehat{\alpha}_j$, $1 \leq j \leq r$, are certain multiples of the α_j's by complex numbers of absolute value less or equal to one. In particular, we can compute the time-frequency parameter (τ_k,ω_k) if the associated attenuation coefficient α_k is sufficiently large, i.e., it appears as a "peak" of $\mathcal{A}(\varphi, H(\varphi))$.

*Definition II-C.1 (δ-**peak**):* Let $\delta > 0$. We say that at $v \in V$ the ambiguity function of f and g has δ-peak, if

$$|\mathcal{A}(f,g)[v]| \geq N^{-1/2+\delta}.$$

Below we describe—see Figure 2—the PR method.

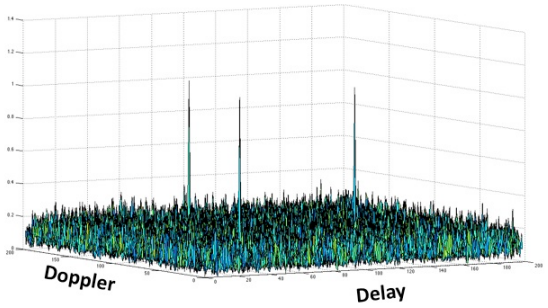

Fig. 2. Profile of $\mathcal{A}(S,R)$ for a pseudo-random sequence S, and a channel of sparsity three.

Pseudo-Random Method

Input: Pseudo-random sequence $S \in \mathcal{H}$, the echo R, and a parameter $\delta > 0$.

Output: Channel parameters.

Compute $\mathcal{A}(S,R)$ on V and return those time-frequency shifts at which the δ-peaks occur.

We call the above computational scheme the **PR method with parameter** δ.

Notice that the arithmetic complexity of the PR method is $O(N^2\log N)$, using Remark II-A.1.

III. Performance of the PR Method

First, we introduce two important quantities that measure the performance of a detection scheme. These are the probability of detection and the expected number of false targets. Then, we formulate the main result of this note which provides a quantitative statement about the performance of the PR method.

Assume that we have r targets out of the N^2 possible—see Section I-A. Also, assume that some random data is associated with these targets and influencing the performance of a detection scheme. For example, in our setting the random data consists of (i) the attenuation coefficients associated with the targets, and (ii) the noise. In general, we model the randomness of the data by associating a probability space $(\mathbf{\Omega}, P)$ to the set of targets. For every $\boldsymbol{\omega}$ in the space $\mathbf{\Omega}$ we denote by $\mathcal{N}_t(\boldsymbol{\omega})$ and $\mathcal{N}_f(\boldsymbol{\omega})$, the number of true and false targets detected by the scheme, respectively. We define the *probability of detection* by

$$P_D = P(\text{a true target is detected}) = \frac{1}{r}\int_{\mathbf{\Omega}} \mathcal{N}_t(\boldsymbol{\omega}) dP(\boldsymbol{\omega}),$$

and the *expected number of false targets* by

$$E_{FT} = E(\mathcal{N}_f) = \int_{\mathbf{\Omega}} \mathcal{N}_f(\boldsymbol{\omega}) dP(\boldsymbol{\omega}).$$

The main result of this note is the following:

*Theorem III-.1 (**Performance of PR method**):* Assume the channel operator (I-A.2) satisfies the uniformity, square root cancellation, and independence assumptions. Then for $r \leq N^{1-\delta}$, where $\delta > 0$, we have $P_D \to 1$, and $E_{FT} \to 0$, as $N \to \infty$, for the PR method with parameter $\delta/4$.

*Remark III-.2 (**Rate of convergence**):* We suspect that the true rate of convergence in $P_D \to 1$, and $E_{FT} \to 0$, as $N \to \infty$, is polynomial. In fact, our proof of Theorem III-.1 confirms that the rate of convergence is at least polynomial.

IV. Conclusions

The obtained estimates in Theorem III-.1 show that the PR method is effective in terms of performance of detection, in the regime $r \leq N^{1-\delta}$, for $\delta > 0$. We would like to note that if $r \geq N^{1+\varepsilon}$, for $\varepsilon > 0$, then the performance of the PR method deteriorates since the noise influence becomes dominant.

V. Proof of Theorem III-.1

Before giving a formal proof, we provide a sketch. To detect the parameters of the channel operator H, the PR method evaluates the ambiguity function of R, and S at v_k:

$$\mathcal{A}(S,R)(v_k) = \alpha_k + \sum_{j\neq k} \alpha_j \langle \pi(v_k)S, \pi(v_j)S\rangle + \langle \pi(v_k)S, \mathcal{W}\rangle.$$

Let us denote by $c_k = \sum_{j\neq k} \alpha_j \langle \pi(v_k)S, \pi(v_j)S\rangle$ the k-th cross term, and by $\nu_k = \langle \pi(v_k)S, \mathcal{W}\rangle$ the k-th noise component. Then we have

$$\mathcal{A}(S,R)(v_k) = \alpha_k + c_k + \nu_k. \tag{V-.1}$$

The parameter v_k is detectable by the PR method if the main term α_k is much larger than the k-th cross term c_k, and the noise component ν_k. For a random point on the unit sphere $S_{\mathbb{C}}^{r-1}$, by "concentration" most of its coordinates are of absolute value approximately equal to $1/\sqrt{r}$. Thus, if $r \leq N$, the magnitude of most of α_k's is greater than $1/\sqrt{N}$. Another instance of the concentration phenomenon guarantees that for most channels, the magnitude of the cross term c_k is smaller than $1/\sqrt{N}$. Finally, the square root cancellation assumption on the noise guarantees that the magnitude of the noise term ν_k is much smaller than $1/\sqrt{N}$.

We begin the formal proof of the theorem with auxiliary lemmata. In Section VI we prove these statements.

*Lemma V-.1 (**Largeness of a slice**):* Let $(\alpha_1, \ldots, \alpha_r)$ be a uniformly chosen point on $S_{\mathbb{C}}^{r-1}$, and fix $k \in \{1, \ldots, r\}$. There exists $K > 0$ (independent of r and k), such that for every $\varepsilon > 0$ we have

$$P\left(|\alpha_k| \geq \varepsilon\right) \geq 1 - K\sqrt{r}\varepsilon.$$

*Lemma V-.2 (**Intersectivity**):* Let $E_1, \ldots, E_r$ be events in a probability space $(\mathbf{\Omega}, P)$, such that $P(E_k) \geq 1 - r^{-\delta}$, $k = 1, \ldots, r$, for some $\delta > 0$. Then for the event

$$E = \{\boldsymbol{\omega} \in \mathbf{\Omega} \mid \boldsymbol{\omega} \text{ is in at least } n(r,\delta) \text{ of } E_k\text{'s}\},$$

where

$$n(r,\delta) = \lfloor (1 - r^{-\delta/2})r \rfloor,$$

we have

$$P(E) \geq 1 - r^{-\delta/2}.$$

*Lemma V-.3 (**Almost orthogonality**):* Let $\ell > 0$, and let $\vec{z_j} = (z_1^j, \ldots, z_r^j) \in \mathbb{C}^r$, $j = 1, \ldots, r^\ell$, be vectors satisfying

$$\sum_{k=1}^{r} |z_k^j|^2 \leq C^2 \frac{r}{N}, \text{ for some } C > 0.$$

Then for any $\delta > 0$, there exists $\beta > 0$, such that for a uniformly chosen random point $\vec{\alpha} \in S_{\mathbb{C}}^{r-1}$ we have

$$P\left(\bigcap_{j=1}^{r^\ell} \left\{ |\langle \vec{\alpha}, \vec{z_j}\rangle| \leq \frac{Cr^\delta}{\sqrt{N}} \right\}\right) \geq 1 - e^{-\beta r^{2\delta}}.$$

***Proof of Theorem III-.1.**:* Assume that $r \leq N^{1-\delta}$, for some $\delta > 0$. Let $R = HS + \mathcal{W}$, where S is a $(B = 1)$-pseudo-random sequence in $\mathcal{H}$, H is a channel of sparsity r with uniformly distributed attenuation coefficients given by (I-A.2), and $\mathcal{W}$ satisfies the square root cancellation assumption. We denote $v_k = (\tau_k, \omega_k), k = 1, \ldots, r$, and assume that at the receiver we perform PR method with parameter $\delta/4$.

(A) Proof of "$P_D \to 1$ as $N \to \infty$".

We consider two cases.

Case 1. $r \geq \log N$.

Denote by $E_k = \{\boldsymbol{\omega} \in \mathbf{\Omega} \mid |\alpha_k(\boldsymbol{\omega})| \geq N^{-1/2+\delta/3}\}$ for $k = 1, \ldots, r$. Since $r \leq N^{1-\delta}$ by Lemma V-.1 there exists $K > 0$ such that we have

$$P(E_k) \geq 1 - Kr^{-\frac{\delta/6}{1-\delta}}.$$

Therefore, for sufficiently large N, we have

$$P(E_k) \geq 1 - r^{-\frac{\delta/7}{1-\delta}}.$$

Denote by

$$E = \{\boldsymbol{\omega} \in \mathbf{\Omega} \mid \boldsymbol{\omega} \text{ is in at least } (1 - r^{-\frac{\delta}{14(1-\delta)}})r \text{ of } E_k\text{'s}\}.$$

By Lemma V-.2 we have

$$P(E) \geq 1 - r^{-\frac{\delta}{14(1-\delta)}}. \tag{V-.2}$$

Since $r \leq N^{1-\delta}$, we have $r^{\frac{\delta/5}{1-\delta}} \leq N^{\delta/5}$. Therefore, by Lemma V-.3, there exists $\beta > 0$ such that

$$P\left(\bigcap_{k=1}^{r}\left\{\left|\sum_{j\neq k}\alpha_j\langle\pi(v_k)S,\pi(v_j)S\rangle\right| \leq N^{-\frac{1}{2}+\frac{\delta}{5}}\right\}\right)$$

$$\geq 1 - e^{-\beta r^{\frac{2\delta}{5(1-\delta)}}}. \tag{V-.3}$$

It follows from (II-C.1), (V-.2), (V-.3), the square root cancellation and independence assumptions, that with probability greater or equal than $1-r^{-\frac{\delta}{15(1-\delta)}}$, at least $(1-r^{-\frac{\delta}{14(1-\delta)}})r$ of the channel parameters of H are detectable.

The latter implies that $P_D \geq (1-r^{-\frac{\delta}{15(1-\delta)}})(1-r^{-\frac{\delta}{14(1-\delta)}})$ for N sufficiently large. Therefore we have $P_D \to 1$ as $N \to \infty$.

Case 2. $r \leq \log N$.

By Lemma V-.1, there exists $K > 0$ such that

$$P\left(\bigcap_{k=1}^{r}\left\{|\alpha_k| \geq N^{-1/2+\delta/3}\right\}\right) \geq 1 - K(\log N)^{3/2}N^{-1/2+\delta/3}.$$

By Cauchy-Schwartz inequality we have for all $k = 1, \ldots, r$:

$$\left|\sum_{j\neq k}\alpha_j\langle\pi(v_k)S,\pi(v_j)S\rangle\right| \leq \frac{\sqrt{r}}{\sqrt{N}} \leq \sqrt{\frac{\log N}{N}}.$$

It follows from (II-C.1), square root cancellation assumption on the noise, and the last two inequalities that for sufficiently large N, all r channel parameters of the operator H are detectable with probability greater or equal than $1 - N^{-1/2+\delta/2}$. Therefore, for sufficiently large N we have

$$P_D \geq 1 - N^{-1/2+\delta/2}.$$

The latter implies that $P_D \to 1$ as $N \to \infty$.

(B) Proof of "$E_{FT} \to 0$ as $N \to \infty$".

Case 1. $r \geq N^{\delta/3}$.

By Lemma V-.3, there exists $\beta > 0$ such that we have

$$P\left(\bigcap_{v\notin supp(H)}\left\{\left|\sum_{k=1}^{r}\alpha_k\langle\pi(v)S,\pi(v_k)S\rangle\right| \leq N^{-\frac{1}{2}+\frac{\delta}{5}}\right\}\right)$$

$$\geq 1 - e^{-\beta r^{\frac{2\delta}{5(1-\delta)}}},$$

where $supp(H) \subset V$ is the set of all channel parameters of H. It follows from (II-C.1), the square root cancellation and independence assumptions, and the last inequality that with probability greater or equal than $1-e^{-\frac{\beta}{2}r^{\frac{2\delta}{5(1-\delta)}}}$ the PR method will not detect any wrong channel parameters. The latter implies that $E_{FT} \to 0$ as $N \to \infty$.

Case 2. $r \leq N^{\delta/3}$.

By Cauchy-Shwartz inequality we have that for every $v \notin supp(H)$:

$$\left|\sum_{k=1}^{r}\alpha_k\langle\pi(v)S,\pi(v_k)S\rangle\right| \leq \frac{\sqrt{r}}{\sqrt{N}} \leq N^{-1/2+\delta/6}.$$

It follows from (II-C.1), the square root cancellation assumption on the noise, and the last inequality that there exists $c > 0$ such that for N sufficiently large we have

$$P\left(\bigcap_{v\notin supp(H)}\left\{|\langle\pi(v)S,R\rangle| < N^{-1/2+\delta/5}\right\}\right) \geq 1 - e^{-cN}.$$

The latter implies that the PR method with parameter $\delta/4$ satisfies $E_{FT} \to 0$ as $N \to \infty$. ∎

VI. Proofs of Lemmata

Proof of Lemma V-.1: We identify the Borel probability space on $S_{\mathbb{C}}^{r-1}$ invariant under all rotations with the Borel probability space S^{2r-1} of the real unit sphere invariant under all rotations. Recall that

$$S^{2r-1} = \{(x_1, y_1, x_2, y_2, \ldots, x_r, y_r) \in \mathbb{R}^{2r} \mid \sum_{k=1}^{r} x_k^2 + y_k^2 = 1\}.$$

Without loss of generality, it is enough to prove the statement for $k = 1$. Let $\alpha_1 = x_1 + i \cdot y_1$. We use the notation $(\boldsymbol{\Omega}, P)$ for the probability space on S^{2r-1} invariant under all rotations in $\mathbb{R}^{2r}$. For any $\rho > 0$, and any dimension n, we denote the real sphere of radius ρ in $\mathbb{R}^n$ by S_ρ^{n-1}:

$$S_\rho^{n-1} = \{(t_1, \ldots, t_n) \in \mathbb{R}^n \mid \sum_{k=1}^{n} t_k^2 = \rho^2\}.$$

Let $\varepsilon > 0$. By Fubini's theorem and using the homogeneity of the Lebesgue measure we get

$$P(\boldsymbol{\omega} \in \boldsymbol{\Omega} \mid |x_1(\boldsymbol{\omega})| \leq \varepsilon)$$

$$= \frac{2}{Area(S_1^{2r-1})} \cdot \int_0^\varepsilon Area(S_{\sqrt{1-t^2}}^{2r-2})dt$$

$$= 2\frac{Area(S_1^{2r-2})}{Area(S_1^{2r-1})}\int_0^\varepsilon (1-t^2)^{\frac{2r-2}{2}}dt.$$

It is well known that

$$\frac{Area(S_1^{n-1})}{Area(S_1^n)} \longrightarrow_{n\to\infty} \sqrt{\frac{n}{2\pi}}.$$

Therefore, for r large enough we have

$$P(\boldsymbol{\omega} \in \boldsymbol{\Omega} \mid |x_1(\boldsymbol{\omega})| \leq \varepsilon) \leq \sqrt{\frac{2(2r-1)}{\pi}}\int_0^\varepsilon (1-t^2)^{r-1}dt$$

$$\leq \sqrt{\frac{4r}{\pi}} \cdot \varepsilon.$$

Finally, the containment $\{\boldsymbol{\omega} \in \boldsymbol{\Omega} \mid |\alpha_1(\boldsymbol{\omega})| \leq \varepsilon\} \subset \{\boldsymbol{\omega} \in \boldsymbol{\Omega} \mid |x_1(\boldsymbol{\omega})| \leq \varepsilon\}$ together with last inequality imply the statement of the lemma. ∎

Proof of Lemma V-.2: Denote by $\gamma = P(E)$, and by $f_k = \chi_{E_k}$, $k = 1, \ldots, r$. Then we have

$$\int \sum_{k=1}^{r} f_k dP \geq r \cdot (1 - r^{-\delta}).$$

On the other hand, we have

$$\int \sum_{k=1}^{r} f_k dP = \int_E \sum_{k=1}^{r} f_k dP + \int_{E^c} \sum_{k=1}^{r} f_k dP$$
$$\leq \gamma \cdot r + (1-\gamma) \cdot (1 - r^{-\delta/2}) \cdot r.$$

The last inequality implies that

$$1 - r^{-\delta} \leq \gamma \cdot r^{-\delta/2} + (1 - r^{-\delta/2}).$$

It implies

$$\gamma \geq 1 - r^{-\delta/2}.$$

■

Proof of Lemma V-.3: Let $\varepsilon > 0$. We proceed similarly to the proof of Lemma V-.1. Since

$$\{\boldsymbol{\omega} \in \boldsymbol{\Omega} \,|\, |\alpha_1(\boldsymbol{\omega})| > \varepsilon\}$$
$$\subset \{\boldsymbol{\omega} \in \boldsymbol{\Omega} \,|\, |x_1(\boldsymbol{\omega})| > \varepsilon/2\} \cup \{\boldsymbol{\omega} \in \boldsymbol{\Omega} \,|\, |y_1(\boldsymbol{\omega})| > \varepsilon/2\},$$

and

$$P(|x_1| > \varepsilon/2) = P(|y_1| > \varepsilon/2) = 2\frac{Area(S_1^{2r-2})}{Area(S_1^{2r-1})} \int_{\varepsilon/2}^{1} (1-t^2)^{r-1}\, dt,$$

we conclude that there exists $K > 0$ such that

$$P(|\alpha_1| > \varepsilon) \leq K\sqrt{r} \int_{\varepsilon/2}^{1} (1-t^2)^{r-1}\, dt.$$

If $\varepsilon = r^{-1/2+\delta}$, then there exists $\beta' > 0$ such that

$$(1 - (\varepsilon/2)^2)^{r-1} \leq e^{-\beta' r^{2\delta}}.$$

This implies that there exists $\beta'' > 0$ such that

$$P(|\alpha_1| \geq r^{-1/2+\delta}) \leq e^{-\beta'' r^{2\delta}}.$$

By the rotation invariance of the Lebesgue measure on S^{2r-1}, it follows that there exists $\beta > 0$ such that for any set of directions $\vec{\theta_1}, \ldots, \vec{\theta_{r^\ell}} \in S^{2r-1}$ we have

$$P\left(\bigcup_{j=1}^{r^\ell} \left\{\boldsymbol{\omega} \in \boldsymbol{\Omega} \,|\, |\langle \vec{\alpha}(\boldsymbol{\omega}), \vec{\theta_j}\rangle| \geq r^{-1/2+\delta}\right\}\right)$$
$$\leq r^\ell \cdot e^{-\beta'' r^{2\delta}} \leq e^{-\beta r^{2\delta}}.$$

The latter implies the statement of the lemma. ■

Acknowledgements. We are grateful to our collaborators A. Sayeed, K. Scheim and O. Schwartz, for many discussions related to the research reported in these notes. Also, we thank anonymous referees for numerous suggestions. And, finally, we are grateful to G. Dasarathy who kindly agreed to present this paper at the conference.

REFERENCES

[1] Fish A., Gurevich S., Hadani R., Sayeed A., and Schwartz O., Delay-Doppler Channel Estimation with Almost Linear Complexity. *IEEE Transactions on Information Theory, Volume 59, Issue 11, 7632-7644, 2013.*

[2] Golomb, S.W., and Gong G., Signal design for good correlation. For wireless communication, cryptography, and radar. *Cambridge University Press, Cambridge (2005).*

[3] Gurevich S., Hadani R., and Sochen N., The finite harmonic oscillator and its applications to sequences, communication and radar . *IEEE Transactions on Information Theory, vol. 54, no. 9, September 2008.*

[4] Howard S. D., Calderbank, R., and Moran W., The finite Heisenberg–Weyl groups in radar and communications. *EURASIP J. Appl. Signal Process (2006).*

[5] Tse D., and Viswanath P., Fundamentals of Wireless Communication. *Cambridge University Press (2005).*

[6] Verdu S., Multiuser Detection, *Cambridge University Press (1998).*