On a system of eigenvectors of the Fourier transform over finite Gaussian fields

A N Karkishchenko\textsuperscript{1} and V B Mnukhin\textsuperscript{1}

\textsuperscript{1}Southern Federal University, Bolshaya Sadovaya 105/42, Rostov-na-Donu, Russia, 344006

e-mail: mnukhin.valeriy@mail.ru

Abstract. The problem of furnishing systems of eigenvectors for the discrete Fourier transform (DFT) is fundamental to image processing with applications in image compression and digital watermarking. This paper studies some properties of such system for DFT over finite fields that may be considered as "finite complex planes". We also considered some applications for multiuser communication schemes.

1. Introduction

The problem of investigating the discrete Fourier transform (DFT) and, especially its eigenstructure, is one of the classical problems of mathematics [1]. Currently such generalizations of DFT as the Hartley transform, the wavelet transform and trigonometric transforms are under intensive study and have numerous applications in digital multiplexing systems design, multiple access systems, error-correcting coding, cryptography, etc [2–4].

Also transforms in finite fields have been intensively studied and applied after Pollard defined the fast Fourier transform in a finite field [5]. In digital signal and image processing these transforms are attractive because they avoid floating point operations and rounding errors. As a result, in comparison with real-valued mathematical tools, faster hardware implementations could be designed [6–15].

In spite of the fact that eigenstructure of a number of such transforms is in general known [16], a lot of questions are still open. Partly it is related with large dimensions of eigenspaces and with the lack of any canonical bases in it. So the problem of finding systems of eigenvectors with any nice special properties is currently actual [17–22].

Encouraged by the above presented aspects, this paper has the main purpose of introducing a new system of eigenvectors for the discrete Fourier transform over “finite complex fields”, called Gaussian fields. Such eigenvectors have a very simple structure related with subgroups of the multiplicative group of the field and are potentially useful in multiuser communication schemes [2, 4] and image compression [23–28].

The paper is organized as follows. After discussing in the next section some applications of eigenvectors in multiuser communications, we introduce finite Gaussian fields in Section 3 and the number-theoretic Fourier transform in Section 4. Eigenvalues of such cyclic FT are studied in Section 5, where the general form of eigenvectors is shown. Then in Section 6 we introduce subgroup eigenspaces and construct its bases. The paper closes with some concluding remarks in Section 7.
2. Eigenvectors for Multiuser Communication

In this section we will discuss applications of eigenvalue sequences for multiuser communications, see also [2, 4].

Assume that some data for two users (Alice and Bob) must be transmitted through the same digital channel by a sender Sam. For this, Sam choose $F$ to be any linear transform over a finite field with at least two distinct eigenvalues $\alpha$ and $\beta$, $\alpha \neq \beta$. Let A and B be the eigenspaces corresponding to $\alpha$ and $\beta$. The idea of Sam is to use vectors $0 \neq u \in A$ as codewords for Alice and $0 \neq v \in B$ as codewords for Bob. To send the data, Sam forms the message vector $w = u + v$ as in Fig. 1 and transmits it through the channel to Alice and Bob.

Now assume that the information about $F$ is known to both Alice and Bob jointly with the assigned eigenvalues $\alpha$ and $\beta$. To decode the message $w$, they note that $F[w] = \alpha u + \beta v$, and so

$$u = \frac{F[w] - \beta w}{\alpha - \beta}, \quad v = \frac{F[w] - \alpha w}{\beta - \alpha}.$$ 

It is easy to note that the same method can be used for any number of users in assumption that $F$ has enough distinct eigenvalues, though the decoding scheme becomes slightly more complicated. In particular, the discrete Fourier transform over finite fields may be used to communicate with four users. It is also clear that it is not compulsory to use all the eigenvectors in eigenspaces. In fact, more reasonable is to use special systems of eigenvectors with any nice properties, say, with error-correcting abilities.

This paper has the main purpose of introducing a new system of eigenvectors for the discrete Fourier transform over “finite complex fields”, called Gaussian fields. Such eigenvectors have a very simple structure related with subgroups of the multiplicative group of the field and so are potentially useful in multiuser communication schemes.

3. Finite Fields of Gaussian Integers

Let $\mathbb{Z}$ and $\mathbb{C}$ be the ring of integers and the complex field respectively, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be a residue class ring modulo an integer $n \geq 2$, and let $\mathbb{GF}(p^m)$ be a Galois field with $p^m$ elements, where $p$ is a prime and $m > 0$ is an integer.

In number theory [29, Ch. 1.4] a Gaussian integer is a complex number $z = a + bi \in \mathbb{C}$ whose real and imaginary parts are both integers. Note that within the complex plane the Gaussian integers may be seen to constitute a square lattice.

Gaussian integers, with ordinary addition and multiplication of complex numbers, form the subring $\mathbb{Z}[i]$ in the field $\mathbb{C}$. Unfortunately, lack of division in such rings significantly restricts
its applicability to image processing problems [30–33]. So it is natural to look for finite fields, whose properties would be in some respect similar to properties of \( \mathbb{C} \). Note, that if \( p = 4k + 3 \) is a prime, then the polynomial \( x^2 + 1 \) is irreducible over \( \mathbb{Z}_p \). As an immediate corollary, the next definition follows.

**Definition 1.** Let \( p \geq 3 \) be a prime number such that \( p \equiv 3 \pmod{4} \). Then the finite field

\[
\mathbb{C}(p) \overset{\text{def}}{=} \mathbb{Z}_p[x]/(x^2 + 1) \simeq \mathbb{GF}(p^2)
\]

will be called *Gaussian field*. Elements of \( \mathbb{C}(p) \) will be called *discrete Gaussian numbers*.

Thus, Gaussian fields have \( p^2 \) elements, where

\[
p = 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, \ldots .
\]

In particular, there are 87 fields \( \mathbb{C}(p) \) for \( 3 \leq p < 1000 \). Elements of Gaussian fields are of the form \( z = a + bi \), where \( a, b \in \mathbb{Z}_p \) and \( i \) denotes the class of residues of \( x \), so that \( i^2 + 1 = 0 \).

The multiplication and addition in \( \mathbb{C}(p) \) is straightforward, just as notions of the *conjugate* to \( z \) number \( z^* = a - bi \in \mathbb{C}(p) \) and the norm \( N(z) = zz^* = a^2 + b^2 \in \mathbb{Z}_p \). (Note that in \( \mathbb{C}(p) \) the concept of modulus \( |z| = \sqrt{N(z)} \) is not defined.) It is easy to show that \( N(z_1z_2) = N(z_1)N(z_2) \) and \( N(z) = 0 \iff z = 0 \).

### 4. Fourier transform over Gaussian fields

Let \( \mathbb{C}(p) \) be any Gaussian field of a characteristic \( p = 4k + 3 \). Since \( \mathbb{C}(p) \) is finite, its multiplicative group \( \mathbb{C}^+(p) = \mathbb{C}(p) \setminus \{0\} \) is cyclic and generated by a primitive element \( g \). For example, \( g = 2 + 7i \) and \( g = 1 + 19i \) are primitive in \( \mathbb{C}^+(71) \) and \( g = 1 + 5i \) is primitive for \( p = 251 \).

Let \( K = |G| = p^2 - 1 \) and let \((f_0, f_1, \ldots, f_{K-1})\) be a vector of length \( K \) with components \( f_s \in \mathbb{C}(p) \). Note that such vectors are in natural correspondence with functions \( f(z) : \mathbb{C}(p) \to \mathbb{C}(p) \) such that \( f(g^s) = f_s \), and from now on we will identify such functions with vectors \( (f_s) \).

There is another way to consider functions on \( \mathbb{C}(p) \). The group algebra of \( G \) over the field \( \mathbb{C}(p) \) is isomorphic to \( \mathbb{C}(p)[X]/(X^K - 1) \) and so its elements may be considered as “polynomials” in the indeterminate \( X \),

\[
q_f(X) = f_0 + f_1X + f_2X^2 + \cdots + f_{K-1}X^{K-1} \in \mathbb{C}(p)[X]/(X^K - 1).
\]

The vector of coefficients \( f_s \in \mathbb{C}(p) \) defines a function \( f \). Thus, we have the bijection

\[
f \longleftrightarrow q_f(X)
\]

and we will call \( q_f(X) \) the *polynomial* representation of \( f \).

**Definition 2.** Let \( \mathbb{C}(p) \) be a Gaussian field and let \( g \) be any generator of its multiplicative group. Let \( f(z) : \mathbb{C}(p) \to \mathbb{C}(p) \) be a function and let \((f_k)\) be the vector of its values, \( f_k = f(g^k) \). The pair of mutually inverse transforms \( \mathcal{F}_g[f] = F \) and \( \mathcal{F}_g^{-1}[F] = f \), given by

\[
F_w = -\sum_{k=0}^{K-1} f_k g^{kw} , \quad f_k = \sum_{w=0}^{K-1} F_w g^{-kw} ,
\]

will be called *cyclic Fourier transform* (CFT briefly) and its inverse respectively. It can be also defined in symmetrized form by

\[
F_w = i \sum_{k=0}^{K-1} f_k g^{kw} , \quad f_k = i \sum_{w=0}^{K-1} F_w g^{-kw} .
\]
Thus, the vector \( (F_w) \) is the left product of \( (f_k) \) by the Vandermonde matrix

\[
U_g = \begin{pmatrix}
1 & 1 & 1 & 1 & \cdots & 1 \\
1 & g & g^2 & g^3 & \cdots & g^{K-1} \\
1 & g^2 & g^4 & g^6 & \cdots & g^{2(K-1)} \\
1 & g^3 & g^6 & g^9 & \cdots & g^{3(K-1)} \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
1 & g^{K-1} & g^{2(K-1)} & g^{3(K-1)} & \cdots & g^{(K-1)(K-1)}
\end{pmatrix}.
\]

In particular, for \( p = 3 \) and \( K = 8 \) we have \( g^2 = i \), \( g^4 = -1 \) and \( g^7 = -ig = g^{-1} \), so that

\[
U_g = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & g & i & ig & -1 & -g & -i & -ig \\
1 & i & -1 & -i & 1 & i & -1 & -i \\
1 & ig & -i & g & -1 & -ig & i & g \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -g & i & -ig & -1 & g & -i & ig \\
1 & -i & -1 & i & 1 & -i & -1 & i \\
1 & -ig & -i & g & -1 & ig & i & g
\end{pmatrix}.
\]

Note that if \( h \) is another generator for \( G \), then \( h = g^s \) with \( \gcd(s, K) = 1 \). Thus, in the matrices \( U_g \) and \( U_h \) the first rows and columns coincide, while other rows and columns are the same up to the permutation

\[
\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & K-1 \\
\ \ s & 2s \mod K & 3s \mod K & \cdots & K-s \end{pmatrix}.
\]

So in fact CFT does not depend on \( g \), and we will write \( F[f] = F \) briefly.

5. Eigenvectors of the cyclic Fourier transform

Note that \( K \equiv -1 \pmod{p} \). The next results are trivial:

**Lemma 1.** \( U^2 = -I \) and so \( F^4 = I \).

**Thus, eigenvalues of \( F \) are \( 1, i, -1, -i \).**

**Lemma 2.** Eigenvalues of the transform \( F^4 \) are 1 and \( -1 \) of multiplicities \( K/2-1 \) and \( K/2+1 \) respectively. The corresponding eigenspaces have the following systems of vectors as bases

\[
\phi^{(1)}_s = X^s - X^{-s} \quad \text{and} \quad \phi^{(-1)}_h = X^h + X^{-h}, \quad \text{where} \ 0 < s < K/2, \ 0 \leq h \leq K/2.
\]

**Lemma 3.** Let \( F \) be an arbitrary linear transform with an eigenvalue \( \lambda \). Let \( v \) be an eigenvector of \( F^2 \) corresponding to the eigenvalue \( \lambda^2 \). Then \( w = \lambda v + F[v] \) is an eigenvector of \( F \) corresponding to \( \lambda \).

**Proof.** Indeed,

\[
F[w] = F[\lambda v + F[v]] = \lambda F[v] + F^2[v] = \lambda F[v] + \lambda^2 v = \lambda(\lambda v + F[v]) = \lambda w.
\]

The next result follows from the previous lemmata immediately.
Proposition 1. The nonzero vectors
\[ \psi_h^{(\lambda)} = \lambda \phi_h^{(\lambda^2)} + \mathcal{F}\left[\phi_h^{(\lambda^2)}\right], \]
where \( \lambda = 1, i, -1, -i \) and \( 0 \leq h \leq K/2 \),
are eigenvectors of the Fourier transform with \( \lambda \) as the corresponding eigenvalue. In other words, these vectors are
\[ \psi_h^{(1)} = \phi_h^{(1)} + \mathcal{F}\left[\phi_h^{(1)}\right] = X^h - X^{-h} + \mathcal{F}[X^h] - \mathcal{F}[X^{-h}], \]
\[ \psi_h^{(-1)} = -\phi_h^{(1)} + \mathcal{F}\left[\phi_h^{(1)}\right] = -X^h + X^{-h} + \mathcal{F}[X^h] - \mathcal{F}[X^{-h}], \]
\[ \psi_h^{(i)} = i\phi_h^{(-1)} + \mathcal{F}\left[\phi_h^{(-1)}\right] = iX^h + iX^{-h} + \mathcal{F}[X^h] + \mathcal{F}[X^{-h}], \]
\[ \psi_h^{(-i)} = -i\phi_h^{(-1)} + \mathcal{F}\left[\phi_h^{(-1)}\right] = -iX^h - iX^{-h} + \mathcal{F}[X^h] + \mathcal{F}[X^{-h}]. \]

Evidently, not all of the vectors \( \psi_h^{(\lambda)} \) are linearly independent.

6. Subgroup eigenspaces

Note that all subgroups of the cyclic group \( G \) are known: for every integer \( L \geq 1 \) that divides \( K = |G| = p^2 - 1 \), there is the unique subgroup \( H \leq G \) of order \( L \). Moreover, \( H \) is generated by any element \( g^k \in G \) such that \( \gcd(k, K) = K/L \), and there are precisely \( \varphi \) such generators, where \( \varphi \) is the totient function. If
\[ K = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s}, \]
then \( G \) has precisely \( S(p) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_s) \) subgroups. Note that \( 4|S(p) \) and \( S(p) \leq 2(p - 1), \) where the equality holds for \( p = 3 \) when \( S(3) = 4 = 2(p - 1) \). The function \( S(p) \) is slowly growing; in particular, \( S(p) \leq S(911) = 192 \) for \( p < 1000 \).

With a subgroup \( H = \langle g^s \rangle \leq G \) we may associate a function \( \chi_H : \mathbb{C}(p) \to \mathbb{C}(p), \)
\[ \chi_H(z) = \begin{cases} 
1, & z \in H, \\
0, & z \notin H.
\end{cases} \]

Since a subgroup of \( G \) is completely determined by its order, sometimes we will refer to \( \chi_H \) as \( \chi_{|H|} \). As a vector, it is
\[ \left(1, 0, 0, \ldots, 0, 0, 1, 0, 0, \ldots, 0, 0, \ldots \right) \]
and the corresponding polynomial is
\[ 1 + X^s + X^{2s} + \ldots + X^{K-s}. \]

Definition 3. The subspace \( \mathcal{S}_p \subset \mathbb{C}^K(p) \) spanned by all the vectors \( \chi_H \) will be called the subgroup space of \( G \). Its dimension is \( S(p) \).

It occurs that the subgroup space is closed under products, convolutions and the Fourier transform. To show it, note first that the subgroup lattice of \( G \) is distributive with the following join and meet operations: for \( H, L \leq G, \)
\[ H \land L = H \cap L, \quad \text{where} \quad |H \cap L| = \gcd(|H|, |L|), \]
\[ H \lor L = \langle H, L \rangle, \quad \text{where} \quad |H \lor L| = \frac{K}{\gcd(K/|H|, K/|L|)}. \]
The subgroup lattice for the field \( \mathbb{C}(7) \)

For example, the subgroup lattice for the field \( \mathbb{C}(7) \) is shown in Fig. 2.

**Theorem 1.** The subgroup space is closed under products of functions, convolutions and the cyclic Fourier transform: for every \( H, L \leq G \),

\[
\chi_H \cdot \chi_L = \chi_{H \wedge L}, \quad \chi_H \ast \chi_L = |H \wedge L| \chi_{H \vee L}, \quad \mathcal{F}[\chi_H] = |H| \chi_{G/H}.
\]

**Corollary 1.** Let \( H < G \) be a subgroup of \( G \). Then

\[
\psi_H^{(i)} \overset{\text{def}}{=} \chi_H - i|H| \chi_{G/H} \quad \text{and} \quad \psi_H^{(-i)} \overset{\text{def}}{=} \chi_H + i|H| \chi_{G/H}
\]

are eigenvectors of the cyclic Fourier transform corresponding to eigenvalues \( \lambda = i \) and \( \lambda = -i \) respectively.

**Proof.** We consider the case \( \lambda = -i \) first. Note that \( |G| = K = p^2 - 1 \equiv -1 \mod p \). Hence,

\[
\mathcal{F}[\psi_H^{(-i)}] = \mathcal{F}[\chi_H] + i|H| \mathcal{F}[\chi_{G/H}] = |H| \chi_{G/H} + iK \chi_H
\]

\[
= |H| \chi_{G/H} - i \chi_H = -i(\chi_H + i|H| \chi_{G/H}) = -i\psi_H^{(-i)}.
\]

The proof for \( \psi_H^{(i)} \) is similar.

Note that eigenvectors corresponding to \( H \) and \( G/H \) will be the same, up to a factor. Since \( |H| \cdot |G/H| = |G| = K \), we may assume in (1) that \( |H| < \sqrt{K} = \sqrt{p^2 - 1} < p \). It also follows from (1) that

\[
\chi_H = \frac{\psi_H^{(i)} + \psi_H^{(-i)}}{2}, \quad \text{and} \quad \chi_{G/H} = i \frac{\psi_H^{(i)} - \psi_H^{(-i)}}{2|H|}.
\]

Now the main result of the paper can be formulated.

**Theorem 2.** When restricted to the subgroup space, the cyclic Fourier transform has only two eigenvalues \( i \) and \( -i \). The corresponding eigenspaces are of dimensions \( S(p)/2 \) each and their bases are formed by the vectors \( \psi_H^{(i)} \) and \( \psi_H^{(-i)} \), where \( H < G \) and \( |H| < p \).

Note that the eigenvectors \( \psi_H^{(i)} \) and \( \psi_H^{(-i)} \) can be naturally visualized in pseudocolours as functions in the “finite complex plane” \( \mathbb{C}(p) \). Examples for \( p = 71 \), when \( K = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \), are in Fig. 3, where blue dots correspond to \( \chi_H \), yellow dots correspond to \( \chi_{G/H} \), and the intersection of terms is marked by red dots.
7. Conclusion
This paper proposes a new system of eigenvectors for the discrete Fourier transform over finite Gaussian fields. Such eigenvectors have a very simple structure related with subgroups of the multiplicative group of the underlying finite field. Subspace spanned by the eigenvectors are closed under products, convolutions and the DFT.

However, apart from this work, there remain issues such as the detailed study of properties of the introduced transformations, the study of possibilities of its generalizations, as well as the details of its practical applications in multiuser communication schemes and image compression. Authors hope to return to the study of these issues in the further papers.
8. References

[1] Auslender L and Tolimieri R 1979 Bull American Math Soc 1 847-897
[2] de Souza R C, de Oliveira H and Cintra R 2017 Multiuser communication based on the DFT eigenstructure (Preprint arXiv 1702.01793)
[3] Lima J, de Souza R C and Panario D 2011 Linear Algebra and its Applications 435 1956-1971 (Access mode: http://www.sciencedirect.com/science/article/pii/S0024379511002552)
[4] de Souza R C and de Oliveira H 2006 Proc. of the 6th International Telecommunications Symposium (Fortaleza-Ce, Brazil, September 3-6) 989-994 (Access mode: 10.1109/ITS.2006.4433415)
[5] Pollard J M 1971 Mathematics of Computation 25 365-374
[6] Bhattacharya M, Creutzburg R and Astola J 2004 Proc. Int. TICS Workshop on Spectral Methods and Multirate Signal Processing
[7] Chandra S S and Svalbe I D 2009 Digital Image Computing: Techniques and Applications 361-368
[8] Chernov V and Korepanov A 2006 Number theoretic transforms in digital image processing (Samara: SGAU) (in Russian)
[9] Chernov V 2007 Arithmetic methods for fast algorithms for discrete orthogonal transforms development (Moscow: FIZMATLIT) (in Russian)
[10] Chernov V and Kasparyan M 2013 Discrete orthogonal transforms on fundamental domains of canonical number systems Computer Optics 37(4) 484-488
[11] Labunets 1982 fiumber fiheoretic fiiransforms over fiuadratic fiields iev: institute of Cybernetics USSR) 30-37 (in Russian)
[12] Varitschenko L, Labunets V and Rakov M 1986 Abstract Algebraic Systems and Digital Signal Processing (Kiev: Naukova Dumka) (in Russian)
[13] Labunets V, Kokh E and Ostheimer E 2018 Algebraic models and methods of computer image processing. Part 1. Multilevel models of multichannel images Computer Optics 42(1) 84-95 DOI: 10.18287/2412-6179-2018-42-1-84-95
[14] Chernov V 2018 Calculation of Fourier-Galois transforms in reduced binary number systems Computer Optics 42(3) 495-500 DOI: 10.18287/2412-6179-2018-42-3-495-500
[15] Boussakta S and Holt A 1999 Advances in Imaging and Electron Physics 111 1-90
[16] McClellan J and Parks T 1972 IEEE Transactions on Audio and Electroacoustics 20 66-74
[17] Horn B K 2010 Transactions of the Royal Society of South Africa 65 100-106 DOI: 10.1080/0035919X.2010.510665
[18] Fendler G and Kaiblinger N 2013 Linear Algebra and Its Applications 438 288302 DOI: 10.1016/j.laa.2012.07.034
[19] Santhanam B and Santhanam T 2008 Signal Processing 88 2738-2746 DOI: 10.1016/ j.sigpro.2008.05.016
[20] Santhanam B and Santhanam T 2007 IEEE International Conference on Acoustics, Speech and Signal Processing 3 1385-1388
[21] de Oliveira Neto J, Lima J and Panario D 2018 Signal Processing
[22] Karkishchenko A and Mnukhin V 2014 Journal of Machine Learning and Data Analysis 1 966-987 (in Russian)
[23] Karkishchenko A and Mnukhin V 2017 Analysis of Images, Social Networks and Texts: 5th International Conference (Communications in Computer and Information Science) 661 281-292
[24] Karkishchenko A and Mnukhin 2016 Proceedings of the First International Scientific Conference Intelligent Information Technologies for Industry (Advances in Intelligent Systems and Computing) 451 153-162
[25] Mnukhin V 2014 Pattern Recognition and Image Analysis 24 552-560
[26] Vybornova Y and Sergeev V 2017 A new watermarking method for vector map data Computer Optics 41(6) 913-919 DOI: 10.18287/2412-6179-2017-41-6-913-919
[27] Rubis A, Lebedev M, Vizilter Y and Vygolov O 2016 Morphological image filtering based on guided contrasting Computer Optics 40(1) 73-79 DOI: 10.18287/2412-6179-2016-40-1-73-79
[28] Gashnikov M, Glumov N, Kuznetsov A, Mitekin V, Myasnikov V and Sergeev V 2016 Hyperspectral remote sensing data compression and protection Computer Optics 40(5) 689-712 DOI: 10.18287/2412-6179-2016-40-5-689-712
[29] Mnukhin V 2013 Journal of Machine Learning and Data Analysis 1 542-551 (in Russian)
[30] Karkishchenko A and Mnukhin V 2013 Bulletin of the Rostov State Transport University 3 147-153 (in Russian)
[31] Mnukhin V 2013 Proc. of the 11th Int. Conf. “Pattern Recognition and Image Analysis: New Information Technologies” (PRIA-11-2013) Pattern Recognition and Image Analysis 11 102-105

Acknowledgements
This research has been partially supported by the Russian Foundation for Basic Research grants no. 16-07-00648 and 17-20-02017. The authors would like to thank the anonymous referee for constructive comments and suggestions.