NOVA

University of Newcastle Research Online

nova.newcastle.edu.au

Hyder, Mashud; Mahata, Kaushik "Zadoff-Chu sequence design for random access initial uplink synchronization in LTE-like systems". Published in IEEE Transactions on Wireless Communications Vol. 16, Issue 1, p. 503-511 (2017)

Available from: <http://dx.doi.org/10.1109/TWC.2016.2625319>

© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting /republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Accessed from: <http://hdl.handle.net/1959.13/1344866>

Zadoff-Chu sequence design for random access initial uplink synchronization in LTE-like systems

Md Mashud Hyder and Kaushik Mahata

Abstract—A Zadoff-Chu (ZC) sequence is uncorrelated with a non-zero cyclically shifted version of itself. However, this alone is insufficient to mitigate inter-code interference in LTE initial uplink synchronization. The performance of the state of the art algorithms vary widely depending on the specific ZC sequences employed. We develop a systematic procedure to choose the ZC sequences that yield the optimum performance. It turns out that the procedure for ZC code selection in LTE standard is suboptimal when the carrier frequency offset (CFO) is not small.

Index Terms—Random Access, initial synchronization, Zadoff-Chu sequence, sparse representation, OFDMA.

I. INTRODUCTION

LTE employs orthogonal frequency-division multiple access (OFDMA) [1] to mitigate multi-user interference. It requires the uplink signals originating from the user equipments (UEs) to be aligned with the local time and frequency references upon their arrival at the eNodeB. To ensure this all UEs wanting to set up new connections with eNodeB must go through an initial uplink synchronization (IUS) procedure. It is a random access (RA) process which starts with the allocation of a pre-defined set of subcarriers called Physical Random Access Channel (PRACH) in some pre-specified time slots known as a “RA opportunity” [1]. The downlink synchronized UEs willing to commence communication, referred to as the random access terminals (RTs), use this opportunity by transmitting a randomly selected ZC code from a pre-specified codebook via the PRACH. Depending on the locations of the RTs within the radio coverage area, their signals arrive at the eNodeB with different time delays. The eNodeB must detect the transmitted RA codes, and extract the timing and channel power information for each detected code. In this paper we develop systematic procedures of designing ZC codebooks to maximize the detection and estimation performance.

To illustrate the need of our analysis consider a typical LTE system with RA preamble format zero [1, Table 5.7.1-1] and system parameters as defined in Table-III. Total $\tilde{G} = 54$ codes $\{\hat{c}_\ell\}_{\ell=1}^{\tilde{G}}$ are available for contention based random access purpose¹ which are ZC sequences of length M . The u -th root

TABLE I
DETECTION PROBABILITIES FOR 3 IUS USERS. SNR OF THE USERS ARE DISTRIBUTED IN $[0, 15]$ dB. P_s DENOTES THE PROBABILITY OF SUCCESS.

Algorithm	P_s with $r = 2.1$ km					
	$n_{cs} = 13$	15	18	22	26	32
SMUD [6]	0.086	0.374	0.980	0.986	0.988	0.998
SRMD [7]	0.340	0.620	0.950	0.966	0.974	0.996
	P_s with $r = 3.2$ km					
	$n_{cs} = 13$	15	18	22	26	32
SMUD [6]	0.006	0.014	0.080	0.460	0.978	0.996
SRMD [7]	0.040	0.106	0.246	0.760	0.974	0.994

ZC sequence Z^u is given element-wise as [4], [5]

$$Z^u(k) = e^{-i\pi u k(k+1)/M}, \quad k \in \mathcal{M}. \quad (1)$$

where $\mathcal{M} = \{0, 1, \dots, M-1\}$, and u is chosen from Table 5.7.2-4 in [1]. The $(k+1)$ -th element of $\hat{c}_{\ell+1}$ is given by

$$\hat{c}_{k+1, \ell+1} = Z^u \{(k + \ell n_{cs}) \bmod M\}, \quad k \in \mathcal{M}. \quad (2)$$

Here $(\ell \bmod M) := \ell - M \cdot \lfloor \ell/M \rfloor$, with $\lfloor r \rfloor$ denoting the largest integer less than or equal to r . The value of n_{cs} is chosen from the set $\mathcal{Q} = \{0, 13, 15, 18, 22, 26, 32, 38, 46, 59, 76, 93, 119, 167, 279, 419\}$, (see [1, Table-5.7.2-2]). Given u , the codes are generated sequentially by varying $\ell = 0, 1, \dots, \lfloor M/n_{cs} \rfloor - 1$ [2]. For more than $\lfloor M/n_{cs} \rfloor$ RA codes we need multiple roots.

We simulate $K = 3$ active RTs with low CFO. The RTs have 75 channel taps which follow the model detailed in Section-VI. Table-I shows the user detection performances of two state of the art IUS algorithms for two different cell radii: $r = 2.2$ km and $r = 3.2$ km, as functions of n_{cs} . Although we can pick any n_{cs} from $\mathcal{Q}$, results in Table-I reveal that the probability P_s of successful code detection vary widely with n_{cs} . When $r = 2.1$ km, P_s is uniformly poor for both methods for $n_{cs} \leq 15$. In contrast, P_s for both SMUD [6] and SRMD [7] are above 0.9 for $n_{cs} \geq 18$. For $r = 3.2$ km we need $n_{cs} \geq 26$ for good results. This clearly demonstrates the importance of choosing n_{cs} on the performance of algorithms.

To the best of our knowledge, so far, there is no systematic study in the literature addressing the issue. Different IUS algorithms are documented in [6]–[10]. The RA procedure proposed in [3] transmits control and data information in the same “access” slot. Different RA frame formats are proposed in [11]. A training-aided ZC sequence design procedure has been proposed in [12] for the frequency synchronization problem addressing estimation and compensation of CFO between a transmitter and a receiver. The effect of CFO on the autocorrelation property of the ZC sequences has been addressed in

Authors are with the Department of Electrical Engineering, University of Newcastle, Callaghan, NSW-2308, Australia (e-mail: md.hyder@uon.edu.au; Kaushik.Mahata@newcastle.edu.au).

Research is supported by the Australian Research Council under the grant number LP150100757.

¹In practice, there are 64 RA codes available in each cell. However, some codes are reserved for contention free RA [2], [3]. We assume that there are 10 reserve codes.

[13], [14]. A closed-form expression of the autocorrelation between two cyclically shifted ZC sequences in presence of frequency offset has been developed in [14]. The ZC sequence design for the timing synchronization problem has been addressed in [12], [15], [16]. The timing synchronization deals with the estimation of timing offset which arises due to the random propagation delay between eNodeB and user [12]. In other direction such as random convolution [17], the ZC sequences are also used to design circulant sensing matrices. The IUS problem is different, and somewhat more difficult from the frequency and timing synchronization problems. The effects of multiple-access interference (MAI) and unknown multipath channel impulse responses of RTs make the ZC sequence design problem challenging.

We show that the signal received in PRACH is a linear combination of few columns of a known matrix. We show that at low CFO environment the data model allows us to pose the IUS parameter estimation as a sparse signal representation problem on an overcomplete basis [18], [19]. We then apply the compressive sensing theory² to recognize a factor called “matrix coherence” that controls the RA code detection performance. We show that the matrix coherence of the underlying IUS problem depends on the code matrix. We suggest a code matrix design procedure. We then analyze the effect of CFO on the RA code design procedure. We show that the LTE standard based RA code generation procedure is not appropriate in larger CFO environment. Then, we propose a new RA code generation procedure to overcome the difficulty.

II. SIGNAL MODEL

Single RT: Consider an OFDMA LTE system with N samples N_p cyclic prefix samples, and M adjacent PRACH subcarriers [1]. The codebook consists of G codes. At an RA opportunity an RT, say T, picks an integer ℓ uniformly at random from $\{1, 2, \dots, G\}$, and transmits $\hat{c}_\ell$. Since LTE uplink uses single carrier frequency division multiple access (SC-FDMA). The transmitter calculates the M point discrete Fourier transform (DFT) c_ℓ of $\hat{c}_\ell$, and modulates the PRACH subcarriers with the components of c_ℓ . As M is always a prime number in LTE, according to [20], [21],

$$c_{k,\ell} = \tilde{Z}^u(k-1)e^{i2\pi(k-1)(\ell-1)n_{cs}/M}, \quad (3)$$

$$\text{with, } \tilde{Z}^u(k) = \frac{e^{i\pi u u^+ k(u^+ k+1)/M}}{\sqrt{M}} \sum_{m=0}^{M-1} Z^u(m), \quad (4)$$

where u^+ is such that $(uu^+) \bmod M = 1$. Using c_ℓ the RT generates $N + N_p + N_g$ time domain channel symbols [1], where N_g is number of guard symbols. The guard symbols prevent the random access preamble from overlapping with the following subframe at the eNodeB receiver. The value of N_g determines the maximum allowable cell radius. We denote these $N + N_p + N_g$ channel symbols by $\{w(k)\}_{k=-N_p}^{N+N_g-1}$. To construct the channel symbols first calculate

$$s(q) = \frac{1}{\sqrt{N}} \sum_{m=1}^M c_{m,\ell} \exp\{i2\pi j_m q/N\}, \quad q = \mathcal{I}, \quad (5)$$

²Sparse recovery algorithms and theories are generally developed in the research area called “Compressive sensing”.

where j_m is the index of m -th PRACH subcarrier, and $\mathcal{I} := \{0, 1, \dots, N-1\}$. We get w from s as

$$w(k) = \begin{cases} s(k \bmod N), & -N_p \leq k \leq N-1, \\ 0, & N \leq k \leq N+N_g-1, \end{cases} \quad (6)$$

Suppose $h(p)$, $p \in \{0, 2, \dots, P-1\}$ are the uplink channel impulse response (CIP) coefficients between the transmitter T and eNodeB where $P < N_p$ is the channel length. Discarding the cyclic prefix and the guard symbols, let $\{v(k)\}_{k=0}^{N-1}$ be the contribution of T in the symbols received by the eNodeB during the RA opportunity. These are delayed and convoluted version of the transmitted symbols. For $k \in \mathcal{I}$,

$$\begin{aligned} v(k) &= e^{i2\pi k\epsilon/N} \sum_{p=d}^{d+P-1} h(p-d) w(k-p), \\ &= e^{i2\pi k\epsilon/N} \sum_{p=d}^{d+P-1} h(p-d) s\{(k-p) \bmod N\}, \end{aligned} \quad (7)$$

where delay d depends on the distance between T and eNodeB, and ϵ is the CFO (normalized by subcarrier spacing Δf). It is convenient to write above as

$$\tilde{v} := [v(0) \ v(1) \ \dots \ v(N-1)]^\top = \mathbf{K}\mathbf{\Omega}\tilde{h}, \quad (8)$$

where $\mathbf{K}$, $\mathbf{\Omega} \in \mathbb{C}^{N \times N}$ and $\tilde{h} \in \mathbb{C}^N$ are defined as

$$\begin{aligned} \tilde{h} &:= [\mathbf{0}_{1 \times d} \ h(0) \ h(1) \ \dots \ h(P-1) \ \mathbf{0}_{1 \times (N-P-d)}]^\top, \\ [\mathbf{\Omega}]_{k,m} &= s\{(k-m) \bmod N\} \\ \mathbf{K} &= \text{diag}\{1, e^{i2\pi\epsilon/N}, e^{i2\pi 2\epsilon/N}, \dots, e^{i2\pi(N-1)\epsilon/N}\} \end{aligned} \quad (9)$$

Here $\mathbf{0}_{1 \times d}$ is a d -vector with all zeros, $(\cdot)^\top$ denotes transpose, $\text{diag}(\cdot)$ is a diagonal matrix, $[\mathbf{\Omega}]_{k,m}$ is the element of $\mathbf{\Omega}$ at its k -th row and m -th column. Let $\mathbf{F}$ be the $N \times N$ DFT matrix:

$$[\mathbf{F}]_{k,m} = \exp\{-i2\pi(k-1)(m-1)/N\}/\sqrt{N}.$$

From $\tilde{v}$ the eNodeB calculates

$$\mathbf{v} = [\mathbf{F}\tilde{v}]_{j_1} \ \mathbf{F}\tilde{v}]_{j_2} \ \dots \ \mathbf{F}\tilde{v}]_{j_M}]^\top = \mathbf{\Theta}\mathbf{F}\mathbf{K}\mathbf{\Omega}\tilde{h}, \quad (10)$$

where $\mathbf{\Theta}$ is an $M \times N$ row selector matrix such that m -th row of $\mathbf{\Theta}$ is the j_m -th row of the $N \times N$ identity matrix. Note that equation (5) is compactly given in matrix form as

$$\mathbf{s} := [s(0) \ s(1) \ \dots \ s(N-1)]^\top = \mathbf{F}^* \mathbf{\Theta}^\top c_\ell, \quad (11)$$

where $(\cdot)^*$ denotes complex conjugate transpose. Since $\mathbf{F}\mathbf{F}^* = \mathbf{I}$, we have $\mathbf{F}\mathbf{s} = \mathbf{\Theta}^\top c_\ell$ where $\mathbf{I}$ is the identity matrix. Thus by circulant structure of $\mathbf{\Omega}$ [22]

$$\mathbf{F}\mathbf{\Omega}\mathbf{F}^* = \text{diag}(\mathbf{F}\mathbf{s}) = \text{diag}(\mathbf{\Theta}^\top c_\ell) = \mathbf{\Theta}^\top \text{diag}(c_\ell) \mathbf{\Theta}, \quad (12)$$

because the m -th row of $\mathbf{\Theta}$ is the j_m -th row of the $N \times N$ identity matrix. Using $\mathbf{F}^*\mathbf{F} = \mathbf{I}$, (3), and (12) in (10) we get

$$\begin{aligned} \mathbf{v} &= \mathbf{\Theta}\mathbf{F}\mathbf{K}\mathbf{F}^*\mathbf{F}\mathbf{\Omega}\mathbf{F}^*\mathbf{F}\tilde{h} = \mathbf{\Theta}\mathbf{F}\mathbf{K}\mathbf{F}^*\mathbf{\Theta}^\top \text{diag}(c_\ell) \mathbf{\Theta}\tilde{h} \\ &= \mathbf{Q} \text{diag}(\tilde{Z}^u) \mathbf{P}_\ell \mathbf{\Theta}\tilde{h}, \quad \mathbf{Q} = \mathbf{\Theta}\mathbf{F}\mathbf{K}\mathbf{F}^*\mathbf{\Theta}^\top. \end{aligned} \quad (13)$$

$$\mathbf{P}_\ell = \text{diag}\{1, e^{i2\pi(\ell-1)n_{cs}/M}, \dots, e^{i2\pi(M-1)(\ell-1)n_{cs}/M}\}.$$

In Appendix A we show $\mathbf{Q}$ is a circulant matrix, and provide its expression in terms of ϵ . In particular, we note that

$$\mathbf{Q} = \mathbf{I} + \mathbf{H}\epsilon + O(\epsilon^2),$$

$$\text{where } \mathbf{H}_{(k,l)} = \begin{cases} i\pi(1 - 1/N), & k = l, \\ -\frac{\pi e^{i\pi(k-l)/N}}{N \sin(\pi(k-l)/N)}, & k \neq l. \end{cases} \quad (14)$$

The nonzero components of $\tilde{\mathbf{h}}$ are concentrated in the rows with indices in the set $\{d+1, d+2, \dots, d+P\}$, see (9). Let $P_{\max}$ be the maximum value of P , and D be the maximum value of d . Denote $N_1 = P_{\max} + D$. Then, $d+P \leq N_1$. Thus, all rows of $\tilde{\mathbf{h}}$ with indices larger than N_1 are zeros. We can truncate $\tilde{\mathbf{h}}$ to an N_1 dimensional vector and rewrite (13) as

$$\mathbf{v} = \mathbf{Q}\tilde{\mathbf{E}}_l\mathbf{h}, \quad (15)$$

$$\text{where, } \tilde{\mathbf{E}}_l = \text{diag}(\tilde{\mathbf{Z}}^u)\mathbf{P}_l\mathbf{\Theta}\mathbf{F}_{(:,1:N_1)}, \quad \mathbf{h} = \tilde{\mathbf{h}}_{(1:N_1)}$$

$\mathbf{F}_{(:,1:N_1)}$ denotes the submatrix of $\mathbf{F}$ formed by taking its first N_1 columns and $\tilde{\mathbf{h}}_{(1:N_1)}$ denotes the sub-vector of $\tilde{\mathbf{h}}$ consisting of its first N_1 components. Note that $\mathbf{E}_l$ is known to the eNodeB for any ℓ . But, $\mathbf{h}$ is unknown. In fact, eNodeB knows neither d , nor ℓ , nor ϵ .

Multiple RTs: For multiple RTs multiple codes are sent. We assume that the number of UEs transmitting a particular code is at most one. This assumption is justified because: (i) Different scheduling approaches in 3GPP ensure this [1], (ii) G is much larger than the number of RTs. Nevertheless, the proposed formulation can be extended easily when the assumption does not hold (see [23, Sec.-II-B]). Hence under the assumption almost surely the received data $\mathbf{y}$ is of the form

$$\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}, \quad \mathbf{A} = [\mathbf{Q}_1\tilde{\mathbf{E}}_1 \quad \mathbf{Q}_2\tilde{\mathbf{E}}_2 \quad \dots \quad \mathbf{Q}_G\tilde{\mathbf{E}}_G], \quad (16)$$

$$\mathbf{x} := [\mathbf{h}_1^\top \quad \mathbf{h}_2^\top \quad \dots \quad \mathbf{h}_G^\top]^\top,$$

where $\mathbf{e}$ denotes noise, and $\mathbf{h}_\ell$ denotes the channel impulse response (see (15)) contributions of RT sending $\mathbf{c}_\ell$. In particular $\mathbf{h}_\ell = 0$ if no RT sends $\mathbf{c}_\ell$. Similarly $\mathbf{Q}_\ell$ is the CFO contribution of the RT sending $\mathbf{c}_\ell$, and is irrelevant if no RT sends $\mathbf{c}_\ell$. The aim of an IUS algorithm is detecting the code indices of active users, their timing offsets i.e., $\{d_\ell\}$ and channel power. For simplicity of notation in (16), we consider single-root case now. Later we generalize to multiple roots.

III. THE ROLE OF MUTUAL COHERENCE

1) IUS as sparse recovery problem: In this section, we consider the standard case where CFO is negligible compared to the subcarrier frequency spacing [6], [9]. In that case $\mathbf{K} \approx \mathbf{I}$, see below (8). Since $\mathbf{\Theta}\mathbf{\Theta}^\top = \mathbf{I}$, and $\mathbf{F}^*\mathbf{F} = \mathbf{I}$, it follows from (13) that $\mathbf{Q} \approx \mathbf{I}$ for all ℓ . Hence, (16) reduces to

$$\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{e}, \quad \mathbf{A} = [\tilde{\mathbf{E}}_1 \quad \tilde{\mathbf{E}}_2 \quad \dots \quad \tilde{\mathbf{E}}_G]. \quad (17)$$

$\tilde{\mathbf{E}}_\ell$ being known for any ℓ , $\mathbf{A}$ is known. Typically the number of RTs is much smaller than the number of codes G . Hence $\mathbf{h}_\ell = 0$ for a vast majority of the values $\ell \in \{1, 2, \dots, G\}$. Even if $\mathbf{h}_\ell \neq 0$ for some ℓ , most components of that $\mathbf{h}_\ell$ have very small magnitude, hence it is sparse [6]–[8]. This makes $\mathbf{x}$ very sparse. Solving $\mathbf{x}$ from $\mathbf{y}$ is a sparse recovery problem. See [24] for a sparse recovery approach to the IUS problem.

TABLE II
SUCCESSIVE MULTIUSER DETECTION (SMUD) [6]

Initialize: Set $\mathbf{r} = \mathbf{y}$, $\mathbf{B} = []$, threshold κ , $\mathbb{T}_\ell = \emptyset$, for $\ell = 1, 2, \dots, G$
repeat
1. Set $d = 0$.
2. For $\ell = 1 : G$
3. Construct: $\mathbb{I} = \{n : \sqrt{\frac{M}{\mathbf{r}^*\mathbf{r}}} [\tilde{\mathbf{E}}_\ell]^*_{:,n} \mathbf{r} > \kappa; n = 1, 2, \dots, N_1\}$.
4. If $\mathbb{I} \neq \emptyset$, set $d = 1$.
5. Update: $\mathbb{T}_\ell = \mathbb{T}_\ell \cup \mathbb{I}$, and $\mathbf{B} = [\mathbf{B} \quad [\tilde{\mathbf{E}}_\ell]_{:, \mathbb{I}}]$.
6. End for
7. Project $\mathbf{y}$ onto null space of $\mathbf{B}$ i.e, $\mathbf{r} = (\mathbf{I} - \mathbf{B}(\mathbf{B}^*\mathbf{B})^{-1}\mathbf{B}^*)\mathbf{y}$
until ($d = 0$)
8. Set of Active code indices: $\mathbb{U} = \{\ell : \mathbb{T}_\ell \neq \emptyset; \ell = 1, 2, \dots, G\}$.
9. Timing offset for ℓ -th active code: $\hat{d}_\ell = \min \mathbb{T}_\ell$.

2) *Mutual coherence:* IUS code detection being a sparse recovery problem, the related theory suggests that detection performance depends on (i) restricted isometry property (RIP) of $\mathbf{A}$ [25], [26] and/or, (ii) mutual coherence [27], [28] of $\mathbf{A}$. Evaluating RIP of a matrix is a computationally hard in general [29]. The “mutual coherence” $\mu(\mathbf{A})$ of $\mathbf{A}$, defined as [27]

$$\mu(\mathbf{A}) = \max_{i \neq j} \frac{|[\mathbf{A}]_{(:,i)}^* [\mathbf{A}]_{(:,j)}|}{\|[\mathbf{A}]_{(:,i)}\|_2 \|[\mathbf{A}]_{(:,j)}\|_2}, \quad (18)$$

with $[\mathbf{A}]_{(:,i)}$ denoting the i th column of $\mathbf{A}$, is the maximum absolute value of the cross-correlation coefficient between any two columns of $\mathbf{A}$. When $\mu(\mathbf{A})$ is small, the columns of $\mathbf{A}$ look different from each other. Thereby, it increases the ability of sparse recovery algorithms to correctly identify the true representation of a signal. See [27], [28] for the theory.

3) *Role of $\mu(\mathbf{A})$ in existing IUS algorithms:* In this section we illustrate the relevance of minimizing $\mu(\mathbf{A})$ for the class of successive interference cancellation (SIC) algorithms [6]–[8]. These algorithms are popular due to low complexity.

SMUD algorithm: We summarize successive multiuser detection (SMUD) method [6] in Table-II. In Step-2, the algorithm selects a code index $\ell \in \{1, 2, \dots, G\}$. Step-3 computes the correlation of every column of $\tilde{\mathbf{E}}_\ell$ to a residual $\mathbf{r}$. It then constructs the set $\mathbb{I}$ by selecting the column indices of $\tilde{\mathbf{E}}_\ell$ whose correlation values are larger than a threshold κ . In Step-5, the selected column indices are concatenated with set $\mathbb{T}_\ell$ and the selected columns of $\tilde{\mathbf{E}}_\ell$ are concatenated to the matrix $\mathbf{B}$. Step-7 updates the residual $\mathbf{r}$ by projecting $\mathbf{y}$ onto the null space of $\mathbf{B}$. Step-8, decides $\mathbf{c}_\ell$ is active if $\mathbb{T}_\ell \neq \emptyset$.

SRMD algorithm: The successive ranging multiuser detection (SRMD) [7] employs a sliding window technique. Except Step-3, SRMD follows similar steps of Table-II. SRMD computes Step-3 as

$$\mathbb{I} = \arg \max_n \left(\sum_{m=n}^{n+P_{\max}-1} |[\tilde{\mathbf{E}}_\ell]^*_{m,n} \mathbf{r}| \right); n = 1, 2, \dots, N_1 - P_{\max}.$$

We investigate the role played by $\mu(\mathbf{A})$ on SMUD and SRMD via a simple example, where for any two matrices $\mathbf{B} \neq \mathbf{D}$, we extend the definition of mutual coherence in (18):

$$\hat{\mu}(\mathbf{B}, \mathbf{D}) = \max_{j,k} \frac{|[\mathbf{B}]_{(:,j)}^* [\mathbf{D}]_{(:,k)}|}{\|[\mathbf{B}]_{(:,j)}\|_2 \|[\mathbf{D}]_{(:,k)}\|_2}, \quad (19)$$

which is the “block coherence” of $\mathbf{B}$ and $\mathbf{D}$. Using the definitions in (18) and (19), it can be verified that

$$\mu(\mathbf{A}) = \max\{\mu(\tilde{\mathbf{E}}_1), \max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)\}. \quad (20)$$

Example 1: Consider two RTs. RT-1 sends c_1 , while RT-2 sends c_2 . For simplicity, assume $e = 0$ and single-tap channels with values of d are 4 and 6 for RT-1 and RT-2. Hence only 5-th component of $\mathbf{h}_1$ is nonzero. Denote $[\mathbf{h}_1]_{(5)} = \tilde{h}_1$ and $[\mathbf{h}_1]_{(k)} = 0$ if $k \neq 5$. Similarly, $[\mathbf{h}_2]_{(7)} = \tilde{h}_2$ and $[\mathbf{h}_2]_{(k)} = 0$ if $k \neq 7$. By (17) we have

$$\mathbf{y} = [\tilde{\mathbf{E}}_1]_{(:,5)} \tilde{h}_1 + [\tilde{\mathbf{E}}_2]_{(:,7)} \tilde{h}_2. \quad (21)$$

In Step-3 of SMUD algorithm with $\ell = 1$, $n = 5$ and $\mathbf{r} = \mathbf{y}$, by the reverse triangular inequality, we get

$$\begin{aligned} |\mathbf{y}^* [\tilde{\mathbf{E}}_1]_{(:,5)}| &\geq |[\tilde{\mathbf{E}}_1]_{(:,5)}|_2^2 \cdot |\tilde{h}_1| - |[\tilde{\mathbf{E}}_1]_{(:,5)}^* [\tilde{\mathbf{E}}_2]_{(:,7)}| \cdot |\tilde{h}_2| \\ &\geq (M/N) |\tilde{h}_1| - (M/N) \{\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) |\tilde{h}_2|\} \end{aligned} \quad (22)$$

where in the last inequality we use (19) and that the length of every column of $\tilde{\mathbf{E}}_\ell$ is $\sqrt{M/N}$, see (40). Clearly if $\sqrt{M/(\mathbf{y}^* \mathbf{y})} \cdot |\mathbf{y}^* [\tilde{\mathbf{E}}_1]_{(:,5)}| > \kappa$ then SMUD successfully detects RT-1. The probability can be increased by decreasing $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$. We would reach the same conclusion for RT-2 by considering $\ell = 2$, $n = 7$ and $\mathbf{r} = \mathbf{y}$ in SMUD Step-3. While detecting the active codes, we like to ensure that false-detection probability is small. Set $\ell \notin \{1, 2\}$ and $\mathbf{r} = \mathbf{y}$ in SMUD Step-3. Using triangular inequality we get

$$|\mathbf{y}^* [\tilde{\mathbf{E}}_\ell]_{(:,n)}| \leq (M/N) \max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) (|\tilde{h}_1| + |\tilde{h}_2|)$$

If $\sqrt{M/(\mathbf{y}^* \mathbf{y})} |[\tilde{\mathbf{E}}_\ell]_{(:,n)}^* \mathbf{y}| > \kappa$ for any $n \in \{1, \dots, N_1\}$ a false-detection occurs, and the false-detection probability reduces by lowering $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$. Finally, consider $\ell = 1$, $n \neq 5$ and $\mathbf{r} = \mathbf{y}$. Similar calculations give

$$|\mathbf{y}^* [\tilde{\mathbf{E}}_1]_{(:,n)}| \leq (M/N) [\mu(\tilde{\mathbf{E}}_1) |\tilde{h}_1| + \max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) |\tilde{h}_2|].$$

Step-3 of SMUD will select the n -th column of $\tilde{\mathbf{E}}_1$ if $\sqrt{M/(\mathbf{y}^* \mathbf{y})} |[\mathbf{y}^* \tilde{\mathbf{E}}_1]_{(:,n)}| > \kappa$. Consequently, Step-5 will update $\mathbb{T}_\ell$ for $\ell = 1$ and hence Step-8 will declare $\ell = 1$ as active code. This will be a correct code detection indeed. But $n \neq 5$, resulting an incorrect timing offset estimate for RT1. The probability of this error can be reduced by making both $\mu(\tilde{\mathbf{E}}_1)$ and $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$ small. Thus

- The value of block coherence affects both user detection and timing offset estimation performance.
- The value of $\mu(\tilde{\mathbf{E}}_1)$ affects the timing offset estimation performance.

By (20) we see the importance of making $\mu(\mathbf{A})$ small. ■

IV. ZADOFF-CHU SEQUENCE SELECTION FOR SMALL CFO

Next we present some results which form the basis of our ZC code design procedure. We start with single root case.

Single root case: The following result is not only applicable when the RA codebook is based on a single ZC root, but also is useful for codebooks with multiple roots. Define

$$\mathcal{S}(r) = M^{-1} |\sin(\pi r M/N) / \{\sin(\pi r/N)\}|. \quad (23)$$

Theorem 1: If $\tilde{\mathbf{E}}_\ell = \text{diag}(\tilde{Z}^u) \mathbf{P}_\ell \mathbf{O} \mathbf{F}_{(:,1:N_1)}$, then $\mu(\tilde{\mathbf{E}}_\ell) = \mathcal{S}(1)$ for all ℓ . In addition, if $\ell, m \in \{1, 2, \dots, G\}$, and

$$MN_1/N \leq n_{cs} \leq M(N - N_1) / \{N(G - 1)\} \quad (24)$$

then $\hat{\mu}(\tilde{\mathbf{E}}_\ell, \tilde{\mathbf{E}}_m) \leq \mathcal{S}(1)$ for any $\ell \neq m$. Define

$$\zeta(n_{cs}) = \frac{n_{cs} N}{M} - (N_1 - 1) \quad (25)$$

In general, if $n_{cs} \leq \frac{M}{G}$ for some n_{cs} satisfying

$$0.25N(M - 1)^{-1} \leq \zeta(n_{cs}) \leq 0.5N \quad (26)$$

then $\hat{\mu}(\tilde{\mathbf{E}}_\ell, \tilde{\mathbf{E}}_m) \leq \mathcal{B}(\zeta(n_{cs})/N)$, where $\mathcal{B}$ is a monotonically decreasing function over $0.25(M - 1)^{-1} \leq \zeta(n_{cs})/N \leq 0.5$:

$$\mathcal{B}(t) = \begin{cases} \frac{12}{\pi(6 - \pi^2 t^2)(M+1)t}, & \frac{1}{4(M-1)} \leq t \leq \sqrt{2}/\pi, \\ \frac{1}{(M+1)t}, & \sqrt{2}/\pi \leq t \leq 1/2 \end{cases} \quad (27)$$

Proof: See Appendix B. ■

Since $\mu(\tilde{\mathbf{E}}_m) = \mathcal{S}(1)$, $\forall m$, the value of $\mu([\tilde{\mathbf{E}}_1 \dots \tilde{\mathbf{E}}_G])$ can never be below $\mathcal{S}(1)$. This bound is achieved if we take $n_{cs} \geq MN_1/N$ (see (24)), provided that $G \leq n_{cs}^{-1} M(1 - N_1/N) + 1$. Thus by setting $n_{cs} = \lceil MN_1/N \rceil$, we can ensure $\mu([\tilde{\mathbf{E}}_1 \dots \tilde{\mathbf{E}}_G])$ is at its minimum possible value $\mathcal{S}(1)$, while we maximize G . If we are willing to work with a smaller G then we may employ a somewhat larger n_{cs} which results in lower block coherence values $\hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$, $\ell \neq m$. This process of decreasing block coherence by increasing n_{cs} , in expense of having less G results some performance improvement. However, making n_{cs} significantly larger than MN_1/N is not very effective. Equation (27) shows that for large n_{cs} the value of block coherence decreases slowly with increasing n_{cs} . We will demonstrate this using numerical simulations.

Multiple root case: Let $\bar{G}$ be the number of codes needed. If G obtained above is smaller than $\bar{G}$, we must use $v = \lceil \bar{G}/G \rceil$ roots. Denote $\mathbf{E}_\ell^u = \text{diag}(\tilde{Z}^u) \mathbf{P}_\ell \mathbf{O} \mathbf{F}_{(:,1:N_1)}$, which makes the root u explicit in definition. Define $\mathbf{B}_u = [\mathbf{E}_1^u \dots \mathbf{E}_G^u]$. We wish to design the set $\mathcal{U} := \{u_1, u_2, \dots, u_v\}$ of roots such that $\mu(\mathbf{A})$ is minimal, where $\mathbf{A} = [\mathbf{B}_{u_1} \dots \mathbf{B}_{u_v}]$. Using (20) we get,

$$\mu(\mathbf{A}) = \max\{\max_{u \in \mathcal{U}} \mu(\mathbf{B}_u), \max_{\substack{u_r \neq u_t; \\ u_r, u_t \in \mathcal{U}}} \hat{\mu}(\mathbf{B}_{u_r}, \mathbf{B}_{u_t})\}. \quad (28)$$

Choosing n_{cs} and G as above ensures $\mu(\mathbf{B}_u) = \mathcal{S}(1)$ for all u . For $\hat{\mu}(\mathbf{B}_{u_r}, \mathbf{B}_{u_t})$ we see that

$$\max_{\substack{u_r \neq u_t; \\ u_r, u_t \in \mathcal{U}}} \hat{\mu}(\mathbf{B}_{u_r}, \mathbf{B}_{u_t}) = \max_{\substack{\ell, m \in \{1, 2, \dots, G\} \\ u_r \neq u_t; u_r, u_t \in \mathcal{U}}} \hat{\mu}(\mathbf{E}_\ell^{u_r}, \mathbf{E}_m^{u_t}) \quad (29)$$

It can be verified via direct calculations using (37) that

$$\begin{aligned} |[\mathbf{E}_\ell^{u_r}]_k^* [\mathbf{E}_m^{u_t}]_p| &= \frac{1}{N} \left| \sum_{n=0}^{M-1} \exp\left(\frac{j\pi}{M} [(u_t(u_t^+)^2 - u_r(u_r^+)^2)n^2 \right. \right. \\ &\quad \left. \left. + (u_t u_t^+ - u_r u_r^+)n + 2n \left\{ n_{cs}(m - \ell) - (p - k) \frac{M}{N} \right\} \right] \right) \right| \end{aligned}$$

Defining $\zeta_{t,r} = u_t(u_t^+)^2 - u_r(u_r^+)^2$ and $\eta_{t,r} = [u_t(u_t^+) - u_r(u_r^+)]/2$, the above expression can be simplified to

$$|[\mathbf{E}_\ell^{u_r}]_k^* [\mathbf{E}_m^{u_t}]_p| = \frac{1}{N} \left| \sum_{n=0}^{M-1} e^{i \frac{\pi}{M \zeta_{t,r}} [n \zeta_{t,r} + \eta_{t,r} + \vartheta(m, \ell, p, k)]^2} \right|$$

where $\vartheta(m, \ell, p, k) = n_{cs}(m - \ell) - M(p - k)/N$.

Lemma 1: If $u_r \neq u_t$, then $|[\mathbf{E}_\ell^{u_r}]_k^* [\mathbf{E}_m^{u_t}]_p| = \sqrt{M}/N$ provided that C1) M is an odd prime integer, C2) $\zeta_{r,t}$ is an even integer. C3) $\{\eta_{r,t} + \vartheta(\ell, m, p, k)\}/\zeta_{r,t}$ is integer valued. **Proof:** Under C2 and C3, $|[\mathbf{E}_\ell^{u_r}]_k^* [\mathbf{E}_m^{u_t}]_p|$ gets simplified to

$$|[\mathbf{E}_\ell^{u_r}]_k^* [\mathbf{E}_m^{u_t}]_p| = \left| \sum_{n=0}^{M-1} e^{i 2 \pi q n^2 / M} \right| / N,$$

for an integer q , which under C1 equals to $\sqrt{M}/N$ [30]. ■

Remark 1: Given a fixed integer q and odd prime M the sequence $e^{i 2 \pi q n^2 / M}$, $n = 0, 1, \dots, M-1$ is known as the Frank-Zadoff-Chu (FZC) sequence [4], [5], [30].

Therefore, if C1-C3 holds then $\hat{\mu}(\mathbf{E}_\ell^{u_r}, \mathbf{E}_m^{u_t}) = 1/\sqrt{M}$. In LTE system C1 of the Lemma-1 holds. We can fulfill C2 by appropriately choosing $\{u_k\}_{k=1}^v$. However, C3 may not hold for all $k, p \in \{1, 2, \dots, N_1\}$. Nevertheless, for a typical LTE system $1/\sqrt{M} \ll \mathcal{S}(1)$, and finding $\mathcal{U}$ such that

$$\hat{\mu}(\mathbf{E}_\ell^{u_r}, \mathbf{E}_m^{u_t}) \leq \mathcal{S}(1), \quad \forall \ell, m, r, t. \quad (30)$$

is not hard. Thus, we choose the roots $\{u_k\}_{k=1}^v$ such that

$$\mu([\mathbf{B}_{u_1} \quad \mathbf{B}_{u_2} \quad \dots \quad \mathbf{B}_{u_v}]) = \mathcal{S}(1),$$

for which a sufficient condition is (30). From u_r and u_t we can readily compute $\mathbf{E}_\ell^{u_r}$, $\mathbf{E}_m^{u_t}$, and $\hat{\mu}(\mathbf{E}_\ell^{u_r}, \mathbf{E}_m^{u_t})$. Thus we can verify if (30) holds on a computer.

V. EFFECT OF CFO ON ZC SEQUENCE DESIGN

If the CFO is not negligible we need to modify the above strategy of ZC sequence selection. For simplicity we assume all the codes share the same root. The generalization for multiple roots is straightforward. Let the CFO for the code c_ℓ is ϵ_ℓ . Write $\mathbf{H}$ in (16) as $\mathbf{H} = i\pi(1 - 1/N)\mathbf{I} + \hat{\mathbf{H}}$, where

$$\hat{\mathbf{H}}_{(k,l)} = \begin{cases} 0, & k = l, \\ -\frac{\pi e^{i\pi(k-l)/N}}{N \sin(\pi(k-l)/N)}, & k \neq l. \end{cases} \quad (31)$$

Denoting $\bar{\mathbf{h}}_\ell = \mathbf{h}_\ell + i\pi(1 - 1/N)\mathbf{h}_{\ell\epsilon_\ell}$, (16) reduces to

$$\mathbf{y} = \sum_{\ell=1}^G \{\tilde{\mathbf{E}}_\ell \bar{\mathbf{h}}_\ell + \hat{\mathbf{H}} \tilde{\mathbf{E}}_\ell \mathbf{h}_{\ell\epsilon_\ell}\} + \mathbf{e}, \quad (32)$$

where we absorb the $O(\epsilon_\ell^2)$ term in $\mathbf{e}$. Doing so is reasonable because the practical values of $|\epsilon_\ell|$ is below 0.5. Given (32), one may first detect and estimate $\bar{\mathbf{h}}_\ell$, which being a scaled version of $\mathbf{h}_\ell$ does not alter the user detection problem. To apply the detection process efficiently, we select the ZC sequences such that $\mu(\mathbf{A}) = \mathcal{S}(1)$ and at the same time we suppress the effect of the terms $\hat{\mathbf{H}} \tilde{\mathbf{E}}_\ell \mathbf{h}_{\ell\epsilon_\ell}$. We extend Example 1 to justify this approach.

TABLE III
SIMULATION PARAMETERS

Parameters	Notation	Values
Carrier Frequency	f_c	2.5 GHz
Sampling Frequency	f_n	30.72 MHz
Subcarrier Spacing	Δf	1.25 KHz
No. of RA Samples	N	24576
Cyclic Prefix (CP) Samples	N_p	3168
Total PRACH Subcarriers	M	839

Example 2: With CFO in Example 1, by writing $\check{\mathbf{h}}_1 = [\check{\mathbf{h}}_1]_{(5)}$ and $\hat{\mathbf{h}}_1 = [\hat{\mathbf{h}}_1 \epsilon_1]_{(5)}$ eq. (32) reduces to

$$\mathbf{y} = [\tilde{\mathbf{E}}_1]_{(:,5)} \check{\mathbf{h}}_1 + [\tilde{\mathbf{E}}_2]_{(:,7)} \check{\mathbf{h}}_2 + \hat{\mathbf{H}} [\tilde{\mathbf{E}}_1]_{(:,5)} \hat{\mathbf{h}}_1 + \hat{\mathbf{H}} [\tilde{\mathbf{E}}_2]_{(:,7)} \hat{\mathbf{h}}_2$$

In Step-3 of SMUD algorithm with $\ell \notin \{1, 2\}$ and $\mathbf{r} = \mathbf{y}$, by the triangular inequality, we get

$$|\mathbf{y}^* [\tilde{\mathbf{E}}_1]_{(:,5)}| \leq (M/N) \max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) (|\check{\mathbf{h}}_1| + |\check{\mathbf{h}}_2|) + \max_{\substack{\ell \neq m \\ r, k}} \left| [\tilde{\mathbf{E}}_m]_{(:,k)}^* [\hat{\mathbf{H}} \tilde{\mathbf{E}}_\ell]_{(:,r)} \right| (|\hat{\mathbf{h}}_1| + |\hat{\mathbf{h}}_2|) \quad (33)$$

with $r, k \in \{1, 2, \dots, N_1\}$. As before, the probability of false detection can be reduced by making the magnitudes of $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$ and the last term small. ■

The ZC code selection procedure proposed above ensures $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell)$ is small. Now we present a way to make

$$\tilde{\mu} = \max_{\ell \neq m} \max_{r, k} \left| [\tilde{\mathbf{E}}_m]_{(:,k)}^* [\hat{\mathbf{H}} \tilde{\mathbf{E}}_\ell]_{(:,r)} \right|$$

small, where $r, k \in \{1, 2, \dots, N_1\}$ and $m, \ell \in \{1, 2, \dots, G\}$. Note that $\tilde{\mu}$ is monotonic in G . We select G to keep $\tilde{\mu}$ below a desired threshold ξ . Our method consists of the following steps: (i) Using (26) and (27) select the smallest n_{cs} and largest G such that $\max_{\ell \neq m} \hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) \leq \xi$. (ii) Set $u = 1$, and $\tilde{G} = G$, (iii) Keep decreasing $\tilde{G}$ until $\tilde{\mu} \leq \xi$. (iv) Generate $\tilde{G}$ number of ZC sequences by using the u . (v) If more roots are needed then increase $u = u + 1$ and repeat steps (iii)-(v) until the desired number of codes are generated. Since the value of block coherence for multiple roots remains close to $\frac{1}{\sqrt{M}}$ (see Lemma-1), we recommend to set $\xi = v/\sqrt{M}$ where $v \geq 1$. We set $v = 10$ in our simulations.

VI. SIMULATION RESULTS

The LTE parameters used in simulations are given in Table-III. RTs being located at different locations, their signals arrive at the eNodeB with different power levels. We simulate this by letting the signal to noise ratio (SNR) of each RT independent and uniformly distributed in $[0, 15]$ dB. The SNR for ℓ -th RT is defined as $\text{SNR} = 20 \log_{10}(\|\mathbf{v}_\ell\|_2 / \|e\|_2)$ where $\mathbf{v}_\ell$ is the received signal at eNodeB from the RT (see (15)) and e is the noise contribution in (16). At each simulation run the mobile speed s varies in the interval $[0, 25]$ m/s with uniform distribution. The wireless channels are modeled according to Extended Pedestrian A model (EPA) [31] if $s \leq 5$ m/s and Extended Vehicular A model (EVA) whenever $s > 5$ m/s. The set of active RA code indices at a particular random access opportunity is denoted by $\mathcal{L}$, while $\hat{\mathcal{L}}$ denotes

Fig. 1. IUS parameter estimation performances by different algorithms as a function of n_{cs} at low CFO. (c) Probability of successfully detecting users with $r = 2.1$ km, (b) Probability of successfully detecting users with $r = 3.2$ km, (c) RMSE of timing estimation with $r = 2.1$ km, (d) RMSE of timing estimation with $r = 3.2$ km, (e) RMSE of power estimation with $r = 2.1$ km, (f) RMSE of power estimation with $r = 3.2$ km.

be the set of code indices detected. The probability that $\mathcal{L} = \hat{\mathcal{L}}$, denoted by P_s , is used as the detection performance measure. In general, we evaluate performance of the proposed method by generating RA codes using the LTE unrestricted set standard [1, Sec. 5.7.2]. However, the proposed method is also applicable for LTE restricted set standards (see [1, Sec. 5.7.2]). The simulation results obtained by applying SMUD on the unrestricted and restricted set RA codes will be denoted by ‘SMUD: unres’ and ‘SMUD: res’ respectively. As before, the maximum number of channel taps for any RT is 75. Hence the value of N_1 (see eq. (15)) equals to 506 and 731 for wireless cell radius $r_1 = 2.1$ km and $r_2 = 3.2$ km respectively. The results are based on 500 independent Monte-Carlo simulations.

A. Performance evaluation at low CFO

The value of CFO of every RT is uniformly distributed in $[-0.015, 0.015]$. Here we validate the following results:

T1: For a given cell radius, the discussion in Section-III-2 suggests to choose n_{cs} to minimise $\mu(\mathbf{A})$. By (24), the smallest n_{cs} in $\mathcal{Q}$ (defined below (1)) that minimize $\mu(\mathbf{A})$ are 18 and 26 for N_1 equal to 506 and 731 respectively.

T2: The analysis around Theorem-1 shows that we can enhance the user detection performance by increasing n_{cs} because a larger n_{cs} yields smaller block coherence value.

Figure-1 plots the RMSE of IUS parameters for different values of n_{cs} . As can be seen in Figure-1(a), for a cell radius $r = 2.1$ km the values of P_s of all algorithms are very

low for $n_{cs} \leq 15$. The value of P_s is above 0.86 for all algorithms when $n_{cs} \geq 18$. Then P_s increases slowly as n_{cs} increases from 18. Figure-1(b) shows a similar result for $r = 3.2$ km. Figure-1(c) shows the timing offset estimation results for $r = 2.1$ km. The performance of the algorithms for all settings are affected by the choice of n_{cs} . The RMSE of ‘SMUD:unres’ with $K = 10$ is high compared to other settings, and is less affected by n_{cs} . The RMSE for restricted RA codes depends similarly on n_{cs} . The RMSE of power estimation results are shown in Figure-1(e-f). Note that the accuracy can be controlled by choosing suitable value of n_{cs} .

B. Performance evaluation at larger CFO

The value of CFO for every user is drawn from a normal distribution with mean $\mathbf{h} \cdot \tau$ and variance 10^{-4} , where the sign $\mathbf{h}$ takes values in $\{+1, -1\}$ with equal probability. Figure-2 compares the code detection performance of different algorithms when the code matrices are designed by using our proposed method (see Section-V), LTE unrestricted set standards and LTE restricted set standards. The results of applying SMUD on the proposed code matrix is denoted by ‘SMUD: proposed’. We generate the codes with $n_{cs} = 32$. In Figure-2(a) for $r = 2.1$ km the detection performance using proposed code matrices is significantly better than other code matrices. The P_s value of ‘SRMD: unres’ drops below 0.55 when $\tau \geq 0.15$. The P_s value of ‘SRMD: proposed’ and ‘SRMD: res’ are 0.86 and 0.126 respectively for $\tau = 0.5$.

Fig. 2. P_s as a function of CFO mean. Number of active RTs $K = 10$.

Similar results for $r = 3.2$ is shown in Figure -2(b), where the code detection performance for restricted and unrestricted codes deteriorates quickly with increasing τ .

VII. CONCLUSION

In this work, we study the dependency of performance of some state-of-the-art initial uplink synchronization algorithms on the random access (RA) code matrix which has been generated from the Zadoff-Chu (ZC) sequences. We observe that the algorithms can not perform equally for all ZC sequences. We apply the theory of compressive sensing to identify the efficient ZC sequences. Theorem-1 and Section-III provide guideline to choose the efficient ZC sequences at low CFO environment. However, this ZC sequence design method needs modification at larger CFO. Section-V gives a detailed analysis of ZC design procedure at larger CFO environment. The empirical results show that if we design the code matrix by using the proposed method then it increases the performance of state of the art IUS algorithms.

APPENDIX

A. Expression for $\mathbf{Q}$

Since $\mathbf{K}$ in (9) is diagonal we know $\mathbf{F}\mathbf{K}\mathbf{F}^*$ is a circulant matrix, i.e.

$$[\mathbf{F}\mathbf{K}\mathbf{F}^*]_{(k,l)}(\epsilon) = r_{((k-l) \bmod N)}(\epsilon),$$

where r_k is a function of ϵ , and is given by

$$\begin{aligned} r_k(\epsilon) &= \frac{1}{N} \sum_{m=0}^{N-1} [\mathbf{K}]_{(m,m)} e^{-i2\pi km/N} = \frac{1}{N} \sum_{m=0}^{N-1} e^{i2\pi(\epsilon-k)m/N} \\ &= (e^{i2\pi\epsilon} - 1) / (e^{i2\pi(\epsilon-k)/N} - 1) / N. \end{aligned} \quad (34)$$

For $k = 0$ above reduces to

$$\begin{aligned} r_0(\epsilon) &= e^{i\pi\epsilon(1-1/N)} \sin(\pi\epsilon) / \{N \sin(\pi\epsilon/N)\} \\ &= 1 + i\pi(1-1/N)\epsilon + O(\epsilon^2). \end{aligned} \quad (35)$$

using the formula for the Taylor series expansion. For $k \neq 0$

$$r_k(\epsilon) = -\epsilon\pi e^{i\pi k/N} / \{N \sin(\pi k/N)\} + O(\epsilon^2),$$

by the Taylor series formula. Using above observations and (14) we get

$$\begin{aligned} \mathbf{Q} &= \mathbf{\Theta}\mathbf{F}\mathbf{K}\mathbf{F}^*\mathbf{\Theta}^\top = [\mathbf{F}\mathbf{K}\mathbf{F}^*]_{(j_1:j_1+M-1, j_1:j_1+M-1)}(\epsilon) \\ &= \mathbf{I} + \mathbf{H}\epsilon + O(\epsilon^2). \end{aligned} \quad (36)$$

B. Proof of Theorem 1

We call that $\tilde{\mathbf{E}}_\ell = \text{diag}(\tilde{Z}^u) \mathbf{P}_\ell \mathbf{\Theta} \mathbf{F}_{(:,1:N_1)}$. Hence

$$[\tilde{\mathbf{E}}_\ell]_{:,n} = \text{diag}(\tilde{Z}^u) \mathbf{P}_\ell \mathbf{\Theta} \mathbf{F}_{(:,n)}. \quad (37)$$

From [30] we know $\left| \sum_{m=0}^{M-1} Z^u(m) / \sqrt{M} \right| = 1$. Thus from (3) we have $|\tilde{Z}^u(k)| = 1$. So $\text{diag}(\tilde{Z}^u)$ is unitary. Hence

$$|[\tilde{\mathbf{E}}_m]^*_{(:,k)} [\tilde{\mathbf{E}}_\ell]_{(:,p)}| = |\mathbf{F}_{(:,k)}^* \mathbf{\Theta}^* \mathbf{P}_m^* \mathbf{P}_\ell \mathbf{\Theta} \mathbf{F}_{(:,p)}|.$$

By the construction of $\mathbf{P}_\ell$ below (13), (23), and recalling $\mathbf{\Theta}$ consists of $j_1 + 1$ through to $j_1 + M$ th rows of $N \times N$ identity matrix we have

$$\begin{aligned} |[\tilde{\mathbf{E}}_m]^*_{(:,k)} [\tilde{\mathbf{E}}_\ell]_{(:,p)}| &= \left| \frac{1}{N} \sum_{q=0}^{M-1} e^{-i2\pi q [(p-k) - \vartheta(\ell-m)]} \right| \\ &= M \mathcal{S}\{(p-k) - \vartheta(\ell-m)\} / N, \end{aligned} \quad (38)$$

where we define

$$\vartheta = N n_{cs} / M = \zeta(n_{cs}) + N_1 - 1 \leq N/G \quad (39)$$

where second equality follows from (25) and the last inequality follows when $n_{cs} \leq M/G$. Since $\mathcal{S}(0) = 1$, setting $m = \ell$ and $k = p$ in above gives

$$\|[\tilde{\mathbf{E}}_\ell]_{(:,p)}\|_2 = \sqrt{M/N}, \quad \forall p, \ell. \quad (40)$$

We need the following properties of $\mathcal{S}$. The last one is a part of [32, Lemma-2.6]. The rest is shown in [33, Appendix-B].

- 1) $\mathcal{S}$ is nonincreasing over $[0, 1]$,
- 2) $\mathcal{S}$ has a unique maximizer over $r \in [1, N-1]$:

$$\arg \max_{1 \leq r < N-1} \mathcal{S}(r) = 1. \quad (41)$$

- 3) $\mathcal{S}(r) < \mathcal{B}(r/N)$ for every $r \in [r_*, N - r_*]$, provided that $r_* \in [0.25N(M-1)^{-1}, 0.5N]$.

Properties 1 and 2, combined with (18), (38) and (40) give

$$\mu(\tilde{\mathbf{E}}_\ell) = \max_{k \neq p} |\mathcal{S}(k-p)| = \mathcal{S}(1). \quad (42)$$

By the reverse triangle inequality we have

$$|\vartheta(\ell-m) - (p-k)| \geq |\vartheta|\ell-m| - |p-k|. \quad (43)$$

For $k, p \in \{0, 1, \dots, N_1-1\}$ we have $0 \leq |k-p| \leq N_1-1$. For $m, \ell \in \{1, 2, \dots, G\}$ such that $\ell \neq m$, we know $1 \leq |\ell-m| \leq G-1$. Thus if $\vartheta \geq N_1$, then $\vartheta|\ell-m| \geq N_1$, which is more than the maximum value of $|k-p|$. Hence, whenever $\vartheta \geq N_1$

$$|\vartheta(\ell-m) - (p-k)| \geq \vartheta - (N_1-1) = \zeta(n_{cs}), \quad (44)$$

where the last equality follows from (39). Applying triangle inequality gives

$$\begin{aligned} |\vartheta(\ell-m) - (p-k)| &\leq |\vartheta(\ell-m)| + |p-k| \\ &\leq \vartheta(G-1) + (N_1-1) \end{aligned} \quad (45)$$

$$\leq N - N/G + N_1 - 1 \leq N - \zeta(n_{cs}), \quad (46)$$

where the first inequality in (46) uses the constraint $n_{cs} \leq M/G$ and last inequality follows from (39). If (24) holds then (39), (44) and (45) implies that

$$1 \leq |\vartheta(\ell - m) - (p - k)| \leq N - 1, \quad (47)$$

and as $\mathcal{S}(r)$ is even function, (38) (41) and (47) implies that

$$|[\tilde{\mathbf{E}}_m]_{(:,k)}^* [\tilde{\mathbf{E}}_\ell]_{(:,p)}| \leq M\mathcal{S}(1)/N,$$

for $m, \ell \in \{1, 2, \dots, G\}$ such that $\ell \neq m$. However, due to (40) this same as saying $\hat{\mu}(\tilde{\mathbf{E}}_m, \tilde{\mathbf{E}}_\ell) \leq \mathcal{S}(1)$. Then using (20) and (42) we see that $\mu(\mathbf{A}) = \mathcal{S}(1)$ whenever (24) holds.

In addition from (44) and (46) we have

$$\zeta(n_{cs}) \leq |\vartheta(\ell - m) - (p - k)| \leq N - \zeta(n_{cs}). \quad (48)$$

Then by (38) and Property 3, we note for $0.25N(M-1)^{-1} \leq \zeta(n_{cs}) \leq 0.5N$ that $\hat{\mu}(\tilde{\mathbf{E}}_\ell, \tilde{\mathbf{E}}_m) \leq \mathcal{B}(\zeta(n_{cs})/N)$.

ACKNOWLEDGEMENT

The authors would like to thank the editor and anonymous referees for their insightful comments and suggestions.

REFERENCES

- [1] "3rd Generation Partnership Project; technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA); physical channels and modulation (release 10)."
- [2] Q. Wang, G. Ren, and J. Wu, "A multiuser detection algorithm for random access procedure with the presence of carrier frequency offsets in LTE systems," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3299–3312, Sept 2015.
- [3] G. Wunder, P. Jung, and C. Wang, "Compressive random access for post-LTE systems," in *Communications Workshops (ICC), 2014 IEEE International Conference on*, June 2014, pp. 539–544.
- [4] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *Information Theory, IEEE Transactions on*, vol. 18, no. 4, pp. 531–532, Jul 1972.
- [5] R. Frank and S. Zadoff, "Phase shift pulse codes with good periodic correlation properties (corresp.)," *Information Theory, IRE Transactions on*, vol. 8, no. 6, pp. 381–382, October 1962.
- [6] M. Ruan, M. Reed, and Z. Shi, "Successive multiuser detection and interference cancellation for contention based OFDMA ranging channel," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 2, pp. 481–487, 2010.
- [7] C.-L. Lin and S.-L. Su, "A robust ranging detection with MAI cancellation for OFDMA systems," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 937–941.
- [8] L. Sanguinetti and M. Morelli, "An initial ranging scheme for the IEEE 802.16 OFDMA uplink," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 9, pp. 3204–3215, 2012.
- [9] L. Sanguinetti, M. Morelli, and L. Marchetti, "A random access algorithm for LTE systems," *Transactions on Emerging Telecommunications Technologies*, vol. 24, no. 1, pp. 49–58, 2013.
- [10] X. W. L. W. P. Shi, Z. R. Wu, "Research on RACH signal detection algorithm in TD-LTE system," *Applied Mechanics and Materials*, vol. 380–384, pp. 3912–3916, 2013.
- [11] T. A. Levanen, J. Pirskanen, T. Koskela, J. Talvitie, and M. Valkama, "Radio interface evolution towards 5g and enhanced local area communications," *IEEE Access*, vol. 2, pp. 1005–1029, 2014.
- [12] M. Gul, X. Ma, and S. Lee, "Timing and frequency synchronization for OFDM downlink transmissions using Zadoff-Chu sequences," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 3, pp. 1716–1729, March 2015.
- [13] S. Sesia, I. Toufik, and M. Baker, *LTE - the UMTS long term evolution : from theory to practice*. Chichester: Wiley, 2009.
- [14] M. Hua, M. Wang, W. Yang, X. You, F. Shu, J. Wang, W. Sheng, and Q. Chen, "Analysis of the frequency offset effect on random access signals," *Communications, IEEE Transactions on*, vol. 61, no. 11, pp. 4728–4740, November 2013.
- [15] C.-L. Wang, H.-C. Wang, and Y.-H. Chen, "A synchronization scheme based on interleaved partial Zadoff-Chu sequences for cooperative MIMO systems," in *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*, Sept 2013, pp. 1–5.
- [16] J.-C. Guey, "The design and detection of signature sequences in time-frequency selective channel," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, Sept 2008, pp. 1–5.
- [17] K. Li, L. Gan, and C. Ling, "Convolutional compressed sensing using deterministic sequences," *IEEE Transactions on Signal Processing*, vol. 61, no. 3, pp. 740–752, Feb 2013.
- [18] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, pp. 21–30, mar 2008.
- [19] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, pp. 489–509, Feb. 2006.
- [20] S. Beyme and C. Leung, "Efficient computation of dft of zadoff-chu sequences," *Electronics Letters*, vol. 45, no. 9, pp. 461–463, April 2009.
- [21] B. Popovic, "Efficient dft of zadoff-chu sequences," *Electronics Letters*, vol. 46, no. 7, pp. 502–503, April 2010.
- [22] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband*, 1st ed. Academic Press, 2011.
- [23] M. M. Hyder and K. Mahata, "A sparse recovery method for initial ranging in IEEE 802.16 OFDMA systems," *CoRR*, 2015. [Online]. Available: <http://arxiv.org/abs/1505.05935>
- [24] —, "A sparse recovery method for initial uplink synchronization in ofdma systems," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 377–386, Jan 2016.
- [25] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, pp. 4203–4215, Dec. 2005.
- [26] E. J. Candès, J. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics*, vol. 59, pp. 1207 – 1223, Mar. 2006.
- [27] J. Tropp, "Just relax: convex programming methods for identifying sparse signals in noise," *Information Theory, IEEE Transactions on*, vol. 52, no. 3, pp. 1030–1051, March 2006.
- [28] Z. Ben-Haim, Y. Eldar, and M. Elad, "Coherence-based performance guarantees for estimating a sparse vector under random noise," *Signal Processing, IEEE Transactions on*, vol. 58, no. 10, pp. 5030–5043, Oct 2010.
- [29] A. Tillmann and M. Pfetsch, "The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing," *Information Theory, IEEE Transactions on*, vol. 60, no. 2, pp. 1248–1259, Feb 2014.
- [30] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences (corresp.)," *Information Theory, IEEE Transactions on*, vol. 25, no. 6, pp. 720–724, November 1979.
- [31] 3GPP-TS-36.101, "User equipment (UE) radio transmission and reception," *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA)*, 2012.
- [32] E. J. Candès and C. Fernandez-Granda, "Towards a mathematical theory of super-resolution," *Communications on Pure and Applied Mathematics*, vol. 67, no. 6, pp. 906–956, 2014.
- [33] M. M. Hyder and K. Mahata, "Zadoff-chu sequence design for random access initial uplink synchronization," *CoRR*, 2016. [Online]. Available: <http://arxiv.org/abs/1604.01476>