ROBUST COMPRESSIVE SHIFT RETRIEVAL IN LINEAR TIME

Michael Clausen, Frank Kurth

Fraunhofer FKIE, Communication Systems, 53343 Wachtberg, Germany
and
Institute of Computer Science 4, University of Bonn, 53113 Bonn, Germany

ABSTRACT

Suppose two finite signals are related by an unknown cyclic shift. Fast algorithms for finding such a shift or variants thereof are of great importance in a number of applications, e.g., localization and target tracking using acoustic sensors. The standard solution, solving shift finding by maximizing the cross-correlation between the two signals, may be rather efficiently computed using fast Fourier transforms (FFTs). Inspired by compressive sensing, faster algorithms have been recently proposed based on sparse FFTs. In this paper, we transform the shift finding problem into the spectral domain as well. As a first contribution, by combining the Fourier Shift Theorem with the Bézout Identity from elementary number theory, we obtain explicit formulas for the unknown shift parameter. This leads to linear time algorithms for shift finding in the noise-free setting. As a second contribution, we extend this result to the fast recovery of weighted sums of two shifts. Furthermore, we introduce a novel iterative algorithm for estimation of the unknown shift parameter for the case of *noisy* signals and provide a sufficient criterion for exact shift recovery. A slightly relaxed criterion leads to a linear time median algorithm in the noisy setting with high recovery rates even for low SNRs.

Index Terms— Shift Retrieval, Compressive Sensing, Fourier Transform, Bézout Identity, TDE, TOA, TDOA

1. INTRODUCTION

In numerous applications one encounters pairs of time-dependent signals that are related by a time shift. The retrieval of time shifts is often referred to as time delay estimation (TDE), with TOA (estimate the time difference between a transmitted signal and its echo) and TDOA (estimate the time difference of arrival of a signal contained in two sensor signals) as two variants [1]. TDE has a wide range of applications in signal detection, synchronization, localization, and tracking. Examples are acoustic target tracking [2], speaker localization [3], and packet synchronization in ultra wideband wireless transceivers [4].

In this paper, we discuss the following shift retrieval problem. Each instance of this problem consists of two signals: a *reference signal* $\boldsymbol{a} \in \mathbb{C}^N$, which is known in advance and which might be preprocessed. Throughout this paper we assume that $\boldsymbol{a}$ differs from all its proper cyclic shifts. The second signal is the *received signal* $\boldsymbol{b} \in \mathbb{C}^N$ which is a possibly noisy version of a cyclic ℓ-shift of $\boldsymbol{a}$ for an unknown positive shift parameter $\ell < N$. The task is to recover ℓ with a minimum amount of computation time and storage space.

A standard procedure for computing ℓ is to correlate the received signal with all possible shifts of the reference signal in the time domain. The correct shift is the one that maximizes the correlation. This cross-correlation approach has computational complexity $O(N^2)$. More efficient procedures are based on the fact that the cross-correlation vector coincides with the cyclic convolution of $\boldsymbol{a}^*_{-N}$ (the complex conjugate of the time reversed version of the reference signal) with the received signal. By the convolution theorem, the Fourier transform of a convolution is the pointwise product of Fourier transforms: $\mathcal{F}(\boldsymbol{a}^*_{-N} * \boldsymbol{b}) = \mathcal{F}(\boldsymbol{a}^*_{-N}) \cdot \mathcal{F}(\boldsymbol{b})$. Hence

$$\boldsymbol{a}^*_{-N} * \boldsymbol{b} = \mathcal{F}^{-1}(\mathcal{F}(\boldsymbol{a}^*_{-N}) \cdot \mathcal{F}(\boldsymbol{b})) \tag{1}$$

describes an alternative way to compute the cross-correlation vector $\boldsymbol{a}^*_{-N} * \boldsymbol{b}$. Thus shift finding via FFT and IFFT needs only $O(N \log N)$ arithmetic operations. Meanwhile, inspired by compressed sensing techniques, there exists faster algorithms for shift finding. In [5], Hassanieh et al. have designed a linear time algorithm for shift finding by exploiting the fact that the cross-correlation vector is sparse and spikes at the correct time shift. In [6], Andoni et al. proposed a procedure for shift finding whose asymptotic running time is even sublinear in N. Interestingly, although inspired by sparse FFT techniques, this algorithm works completely in the time domain. As the basic algorithm in [6] recovers the true shift ℓ for *binary* signals "with high probability," it remains to study the recovery rate of this TDE algorithm for more general input signals.

The primary goal of this paper is to solve the shift finding problem completely in the spectral domain. This avoids an inverse Fourier transform. In Section 2 we propose an approach for solving this problem in a noise-free scenario. Here, we uncover the close connection between shift retrieval and GCD computations. Combining the Fourier Shift Theorem with Bézout's Identity we obtain several explicit formulas for the unknown shift, resulting in linear time algorithms

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

for shift finding. In Section 3 we extend this technique to the case, where the received signal is a linear combination of two (noise-free) shifts of the reference signal, which has applications in scenarios involving echoes.

The remaining part of this paper discusses shift retrieval in the noisy setting. For ease of presentation, we restrict ourselves to signals of length $N = 2^n$. In Section 4 we propose a novel method for estimating the unknown shift parameter ℓ iteratively. We furthermore provide a sufficient criterion for exact shift recovery. For this iterative estimation we only need from both signals the Fourier coefficients corresponding to indices which are powers of two. All these indices can be computed in linear time. As the sufficient criterion is hard to check in an application scenario, we relax on the one hand this criterion and compensate on the other hand this relaxation by using several noisy versions of the reference signal to attenuate the influence of noise. This results in a linear time median method for shift estimation with high recovery rates (> 90 %) even for low SNRs.

Notation: For a (nonzero) complex number $z \in \mathbb{C}$, $\mathrm{Re}(z)$ denotes its real part, $|z|$ its absolute value, z^* its complex conjugate, and $\arg(z)$, $0 \leq \arg(z) < 2\pi$, its argument or phase. With this notation, $z = |z| \cdot \exp(\mathrm{i} \cdot \arg(z))$. For integers $m \leq n$ let $[m, n] := \{x \in \mathbb{Z} \mid m \leq x \leq n\}$. Finally, we denote by $x \bmod N \in [0, N-1]$ the remainder after division of $x \in \mathbb{Z}$ by $N \in \mathbb{N}$.

2. NOISE-FREE COMPRESSIVE SHIFT RETRIEVAL

This section discusses the noise-free case, i.e., the received signal is a cyclic shift of the reference signal. The goal is to compute the unknown shift efficiently. Theorem 1 below presents two explicit formulas for the unknown shift. These formulas establish a flexible tool for the recovery of the unknown shift in linear time.

Let $\boldsymbol{a} = (a_0, \ldots, a_{N-1})^\top$ and $\boldsymbol{b}$ denote two complex-valued signals of finite length N. Suppose, $\boldsymbol{b}$ is a cyclic shift of $\boldsymbol{a}$, i.e., $b_k = a_{k-\ell \bmod N}$, for an unknown positive shift parameter $\ell < N$. (The signal $\boldsymbol{b}$ is then the *ℓ-shift* of $\boldsymbol{a}$; notation: $\boldsymbol{b} = C_\ell(\boldsymbol{a})$.) To efficiently recover ℓ, we transform the shift finding problem into the spectral domain and consider the Fourier transforms $\boldsymbol{A} = (A_0, \ldots, A_{N-1})^\top$ and $\boldsymbol{B}$ of $\boldsymbol{a}$ and $\boldsymbol{b}$, where

$$A_k = \sum_{n<N} \omega^{k \cdot n} a_n \quad \text{and} \quad B_k = \sum_{n<N} \omega^{k \cdot n} b_n.$$

Here ω denotes a primitive Nth root of unity. We take $\omega := \exp(2\pi \mathrm{i}/N)$. Using $\omega^{m+n} = \omega^{m+n \bmod N}$ and $b_k = a_{k-\ell \bmod N}$, a simple calculation yields the well-known Fourier Shift Theorem: $B_k = A_k \omega^{k\ell}$. If $A_k \neq 0$, we obtain the fundamental equation

$$B_k / A_k = \omega^{k \cdot \ell}. \tag{2}$$

As we are mainly interested in recovering the unknown positive shift parameter ℓ, our next goal is to get rid of the factor k in the exponent. Here, the following fact from elementary number theory turns out to be very useful.

Bézout identity. If $g \in \mathbb{N}$ is the greatest common divisor of the integers $n_1, \ldots, n_r$, then there are integers $n'_1, \ldots, n'_r$ with $g = n_1 n'_1 + \ldots + n_r n'_r$.

For GCD algorithms computing $(g; n'_1, \ldots, n'_r)$ on input $(n_1, ..., n_r)$ in time subquadratic in the bit-lengths, in our case $\log N$, we refer to [7]. Note that in contrast to g the sequence of Bézout coefficients $(n'_1, \ldots, n'_r)$ is not uniquely determined by $(n_1, \ldots, n_r)$. For example, if $(n_1, n_2) = (8, 12)$, then $g = 4$ and both $4 = (-1)\cdot 8 + 1 \cdot 12$ and $4 = 2 \cdot 8 + (-1) \cdot 12$ are possible corresponding Bézout identities. Now we are well-prepared to state our first result.

Theorem 1. Suppose $\boldsymbol{b}$ is the ℓ-shift of $\boldsymbol{a} \in \mathbb{C}^N$ with an unknown positive shift parameter $\ell < N$.
(a) Let $k \in [1, N-1]$ and N be coprime and let $1 = \gcd(k, N) = kk' + NN'$ be a corresponding Bézout identity. If the kth Fourier coefficient A_k is nonzero, then the shift parameter ℓ can be recovered from A_k, B_k, and k' via

$$\ell = \arg((B_k/A_k)^{k'}) \cdot N/(2\pi). \tag{3}$$

(b) Let K denote a nonempty subset of $[1, N-1]$ with $A_k \neq 0$ for all $k \in K$. If the greatest common divisor of all $k \in K$ is 1 and $1 = \sum_{k \in K} kk'$ is a corresponding Bézout identity, then the knowledge of all pairs $(A_k, B_k)_{k \in K}$ and the vector of Bézout coefficients $(k')_{k \in K}$ is sufficient to recover the unknown shift parameter ℓ:

$$\ell = \arg\Big(\prod_{k \in K} (B_k/A_k)^{k'} \Big) \cdot N/(2\pi). \tag{4}$$

Proof. **(a)** With the fundamental equation (2) we obtain $(B_k/A_k)^{k'} = \omega^{k\ell \cdot k'} = \omega^{(1 - NN') \cdot \ell} = \omega^\ell$. As $\arg(\omega^\ell) = 2\pi\ell/N$, (3) is valid.

(b) Applying the fundamental equation (2) again we obtain $\prod_{k \in K} (B_k/A_k)^{k'} = \prod_{k \in K} \omega^{kk' \cdot \ell} = \omega^{\sum_{k \in K} kk' \cdot \ell} = \omega^\ell$. Thus $\arg(\prod_{k \in K} (B_k/A_k)^{k'}) = \arg(\omega^\ell) = 2\pi\ell/N$, hence (4) is valid. □

Theorem 1 simplifies and generalizes the results of Section III in [8], in addition, our result avoids the usual hypothesis testing. Moreover, GCDs are not restricted to positive indices k coprime to N but our result allows, e.g., to work with arbitrary coprime pairs independent of N. This enhances the applicability of compressive sensing considerably. The number of $k \in [1, N-1]$ which are coprime to N (these are the potential candidates in (a)), is given by Euler's totient function φ evaluated at N. It is well-known that $\varphi(N) = N/\prod_p (1 - (1/p))$, where the product runs through all prime divisors p of N. For example, $\varphi(2^n) = 2^{n-1}$, i.e., if N is a power of two, then half of the indices k are candidates for applying Theorem 1(a). Now consider $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$.

Then $\varphi(N) = 1\cdot 2\cdot 4\cdot 6\cdot 10 = 480$. In this case, only 20.8% of the indices k are candidates for applying Theorem 1(a). The next result points to preferable candidate pairs.

Corollary 2. Let $\boldsymbol{a} \in \mathbb{C}^N$ and suppose $\boldsymbol{b} = \lambda \cdot C_\ell(\boldsymbol{a})$ with unknown parameters $0 \neq \lambda \in \mathbb{C}$ and $\ell \in [1, N-1]$. If A_k and A_{k+1} are nonzero, for some $k \in [0, N-2]$, then λ and ℓ can be uniquely recovered from A_k, B_k, A_{k+1}, and B_{k+1}.

Proof. First note that in this case, there is a trivial corresponding Bézout identity: $1 = 1\cdot(k+1) + (-1)\cdot k$. As the Fourier transform is linear, we obtain with equation (2)

$$\frac{B_{k+1}}{A_{k+1}} \cdot \frac{A_k}{B_k} = \frac{\lambda \cdot \omega^{(k+1)\ell} A_{k+1}}{A_{k+1}} \cdot \frac{A_k}{\lambda \cdot \omega^{k\ell} A_k} = \omega^\ell\,,$$

which allows to recover ℓ. Finally, $\lambda = B_k/(\omega^{k\ell} A_k)$. □

Here is a concrete example. Let $N = 12$ and $A_2 \cdot A_3 \neq 0$. As both 2 and 3 are not coprime to 12, Theorem 1(a) is not applicable in contrast to Corollary 2.

3. FAST RECOVERY OF THE WEIGHTED SUM OF TWO SHIFTS

In this section we approach shift retrieval for scenarios where the signal $\boldsymbol{b}$ is the weighted sum of shifted versions of $\boldsymbol{a}$. An important application scenario is the estimation of echo components. To model superimposed shifted signals, we consider signals $\boldsymbol{a}$ and $\boldsymbol{b} = \lambda\cdot C_\ell(\boldsymbol{a}) + \rho\cdot C_r(\boldsymbol{a})$. On input $\boldsymbol{a}$ and $\boldsymbol{b}$ our goal is to recover the unknown positive shift parameters $\ell \neq r$ (both smaller than N) and the unknown positive rational (!) numbers λ and ρ.[1] We start with the case $\lambda = \rho = 1$.

Theorem 3. Suppose $\boldsymbol{b} = C_\ell(\boldsymbol{a}) + C_r(\boldsymbol{a})$ is the sum of two cyclic shifts of $\boldsymbol{a} \in \mathbb{C}^N$ with unknown positive shift parameters $\ell \neq r$ both smaller than N. If $k \in [1, N-1]$ and N are coprime, $1 = kk' + NN'$, and if the kth Fourier coefficient B_k does not vanish, then the unknown shift parameters ℓ and r can be recovered from A_k, B_k, and k' via (3) and formula (5) below.

Proof. As the Fourier transform is linear, we obtain $B_k = A_k \cdot (\omega^{k\ell} + \omega^{kr})$, see (3). By assumption, $B_k \neq 0$, hence both A_k and $\omega^{k\ell} + \omega^{kr}$ do not vanish. After division by A_k we know $0 \neq \omega^{k\ell} + \omega^{kr} =: 2\cdot z$. Now $|z| < 1$ (because $\ell \neq r$) and the line Λ through z, which is perpendicular to the line through the origin and z, intersects the unit circle in $\omega^{k\ell}$ and ω^{kr}. For an illustration see Figure 1.

More precisely, $\Lambda = \{z + x\cdot \mathrm{i}\cdot z \mid x \in \mathbb{R}\}$. Thus we are looking for all $x \in \mathbb{R}$ with $|z + x\cdot \mathrm{i}\cdot z| = 1$. An easy calculation yields the two solutions $x = \pm\sqrt{|z|^{-2} - 1}$. Thus we know both $\omega^{k\ell}$ and ω^{kr}:

$$\{\omega^{k\ell}, \omega^{kr}\} = \{z\cdot(1 \pm \mathrm{i}\cdot\sqrt{|z|^{-2} - 1})\}. \qquad (5)$$

[1] In view of some applications involving radio-frequency (RF) signals, the scaling of shifted signals may be complex-valued. However, positive rational numbers as scalars are crucial in our proof of Theorem 4.

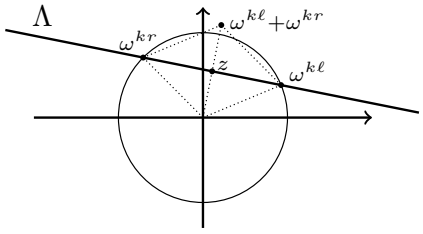

Fig. 1. Fast recovery of the shift parameters ℓ and r.

As k and N are coprime, we can apply formula (3) to recover the unknown shift parameters ℓ and r. □

We generalize Theorem 3. (Recall Euler's totient function.)

Theorem 4. Suppose $\boldsymbol{b} = \lambda\cdot C_\ell(\boldsymbol{a}) + \rho\cdot C_r(\boldsymbol{a})$ is the weighted sum of two shifts of $\boldsymbol{a} \in \mathbb{C}^N$ with unknown positive shift parameters $\ell \neq r$ smaller than $\varphi(N)$ and unknown positive rational (!) numbers λ and ρ. If $k \in [1, N-1]$ and N are coprime and if the Fourier coefficients B_0 and B_k do not vanish, the unknown parameters ℓ, r, λ, and ρ can be uniquely recovered from A_0, B_0, A_k, and B_k in time linear in N.

Proof. By our assumptions we obtain in the spectral domain $0 \neq B_k = A_k\cdot(\lambda\cdot\omega^{k\ell} + \rho\cdot\omega^{kr})$ and $0 \neq B_0 = A_0\cdot(\lambda+\rho)$. Hence $\lambda+\rho = B_0/A_0$ can be recovered. Let $\mu := \lambda/(\lambda+\rho)$. Although μ is unknown, we know that

$$Z := \frac{B_k}{A_k}\cdot\frac{A_0}{B_0} = \mu\cdot\omega^{k\ell} + (1-\mu)\cdot\omega^{kr}$$

is a convex combination with rational coefficients of the unknown roots $\omega^{k\ell}$ and ω^{kr}. Similar to Figure 1, we consider the line Λ through Z which is perpendicular to the line through the origin and Z. In Figure 2, only the corresponding chord of Λ is shown (in black). As Z is a convex combination of two Nth roots of unity, the chord defined by these two roots (shown is green) is either equal to the black chord, in which case $\mu = 1/2$ and we are in the situation of Theorem 3, or the two chords are different. In the latter case, one of the roots we are looking for is among the blue ones. To find the other root, we use Cartesian coordinates. For every blue root $X = (x_1, x_2)$ let $Y = (y_1, y_2)$ denote the point where the ray through $Z = (z_1, z_2)$ starting at X intersects the unit circle. An easy calculation shows that $Y = wZ + (1-w)X$, where $w = v/(\|Z\|^2 - 1 + v)$, $v = 2\cdot(1 - Z\cdot X^\top)$. Looking at the phase, one can check whether Y is another Nth root of unity. As each triple (X, Y, root test) can be processed in constant time, the overall running time is linear in N.

It should be remarked that ℓ and r are uniquely determined as long as ℓ and r are smaller than $\varphi(N)$. This follows from the fact that the roots $1, \omega, \omega^2, \ldots, \omega^{\varphi(N)-1}$ form a $\mathbb{Q}$-basis of the Nth cyclotomic field $\mathbb{Q}(\omega)$, which is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and ω, see, e.g., Chapter VI.3 in [9]. Finally, combining $B_0/A_0 = \lambda + \rho$ with the fact that $|\omega^{k\ell} - Z|/|\omega^{k\ell} - \omega^{kr}| \in \{\mu, 1-\mu\}$ allows us to recover λ and ρ. This concludes the proof of Theorem 4. □

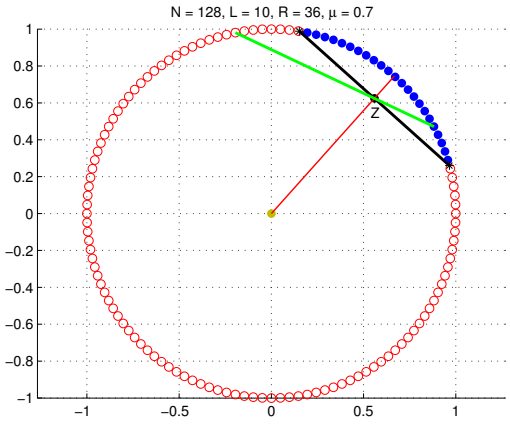

Fig. 2. Fast recovery of the parameters in $\lambda \cdot \omega^{k\ell} + \rho \cdot \omega^{kr}$.

4. NOISY COMPRESSIVE SHIFT RETRIEVAL

In this section we study a noisy version of compressive shift retrieval. More precisely, we assume that $\boldsymbol{a} \in \mathbb{C}^N$ is a noise-free known reference signal whereas $\widetilde{\boldsymbol{b}}$ is a noisy version of $\boldsymbol{b} = C_\ell(\boldsymbol{a})$, $\ell < N$ an unknown positive shift parameter. Thus $\widetilde{\boldsymbol{b}} = \boldsymbol{b} + \boldsymbol{n}$, for some additive noise vector $\boldsymbol{n}$. In the spectral domain we thus have $\widetilde{\boldsymbol{B}} = \boldsymbol{B} + \boldsymbol{N}$. If $A_k \neq 0$, we obtain the following noisy version of the fundamental equation (2)

$$\frac{\widetilde{B}_k}{A_k} = \frac{B_k}{A_k} + \frac{N_k}{A_k} = \omega^{k\ell} + \frac{N_k}{A_k}. \tag{6}$$

Keeping this notation, the next result indicates how to compute the unknown shift parameter ℓ iteratively starting with the least significant bit. Before going into the technical details, we will illustrate the basic idea. Let $N = 2^n$ and $M := N/2$. Suppose $A_M \cdot \widetilde{B}_M \neq 0$ and $|N_M/A_M| < 1$. Then, by (6),

$$\left|\frac{\widetilde{B}_M}{A_M} - \omega^{M\ell}\right| = \left|\frac{N_M}{A_M}\right| < 1. \tag{7}$$

But $\omega^M = -1$, hence $\omega^{M\ell} = (-1)^\ell = (-1)^{\ell \bmod 2}$. Thus in (7), $|\widetilde{B}_M/A_M - (-1)^{\ell \bmod 2}| < 1$. In geometric terms this means that $\widetilde{B}_M/A_M$ lies within the unit circle around $(-1)^{\ell \bmod 2}$. As the two open unit disks around $+1$ and -1 are disjoint, the real part of $\widetilde{B}_M/A_M$ decides on the parity of ℓ: if $\mathrm{Re}(\widetilde{B}_M/A_M) > 0$, i.e., $\widetilde{B}_M/A_M$ is within the green area in Figure 3, then $\ell \bmod 2 = 0$. If $\mathrm{Re}(\widetilde{B}_M/A_M) < 0$, i.e., $\widetilde{B}_M/A_M$ is within the red area, then $\ell \bmod 2 = 1$. It remains to note that $A_M \cdot \widetilde{B}_M \neq 0$ implies $\widetilde{B}_M/A_M \neq 0$.

Define $\ell_m := \ell \bmod 2^m$. We have illustrated above how to compute $\ell_1 = \ell \bmod 2$. Next we iterate this process and compute ℓ_m with the help of ℓ_{m-1}. Keeping the binary representation $\ell = \sum_i b_i 2^i$ in mind it follows that $\ell_m = \ell_{m-1} + b_{m-1} \cdot 2^{m-1}$. Thus $\ell_m = \ell_{m-1}$ or $\ell_m = \ell_{m-1} + 2^{m-1}$.

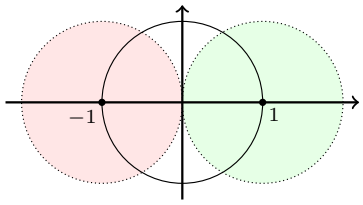

Fig. 3. Computing the least significant bit of ℓ.

Theorem 5. Let $N = 2^n$. Suppose $A_k \cdot \widetilde{B}_k \neq 0$ and $|N_k/A_k| < 1$, for all $k = 2^m$, $m \in [1, n-1]$.
(a) If $k = N/2$ and $p \in \{0, 1\}$ minimizes $|\widetilde{B}_k/A_k - (-1)^p|$, then $\ell \bmod 2 = p$, i.e., $\ell_1 = p$.
(b) Suppose, we already know that $\ell_{m-1} = q$, for some $m \in [2, n]$. If $k = N/2^m$ and $r \in \{q, q + 2^{m-1}\}$ minimizes $|\widetilde{B}_k/A_k - \omega^{kr}|$, then $\ell_m = r$.

Proof. **(a)** See above. **(b)** If $k = N/2^m$, then $\omega^k = \exp(2\pi \mathrm{i}/2^m)$ is a primitive 2^m-th root of unity and (6) yields $|\widetilde{B}_k/A_k - \omega^{k\ell}| = |\widetilde{B}_k/A_k - \omega^{k \cdot (\ell \bmod 2^m)}| = |N_k/A_k| < 1$. By assumption, we already know that $\ell_{m-1} = q$. Hence $\ell_m \in \{q, q + 2^{m-1}\}$. But $|\omega^{kq} - \omega^{k(q+2^{m-1})}| = |\omega^{kq} + \omega^{kq}| = 2$. Now a similar argument as in (a) shows that there is a unique integer $r \in \{q, q + 2^{m-1}\}$ satisfying $|\widetilde{B}_k/A_k - \omega^{kr}| = |N_k/A_k| < 1$. Thus $\ell \bmod 2^m = r$. □

Equivalent but simpler versions of the conditions in **(a)** and **(b)** read as follows.

$$\textbf{(a)}\colon\ \ell_1 = \begin{cases} 0 & \text{if } \mathrm{Re}(\widetilde{B}_{N/2}/A_{N/2}) > 0, \\ 1 & \text{if } \mathrm{Re}(\widetilde{B}_{N/2}/A_{N/2}) < 0, \end{cases}$$

$$\textbf{(b)}\colon\ \ell_m = \begin{cases} \ell_{m-1} & \text{if } \mathrm{Re}((\widetilde{B}_k/A_k) \cdot \omega^{-kq}) > 0, \\ \ell_{m-1} + 2^{m-1} & \text{if } \mathrm{Re}((\widetilde{B}_k/A_k) \cdot \omega^{-kq}) < 0, \end{cases}$$

where $k = N/2^m$ in (b). According to this result, the unknown shift parameter ℓ can be correctly recovered if we know A_k and $\widetilde{B}_k$ for all proper divisors k of N, provided that $A_k \cdot \widetilde{B}_k \neq 0$ and $|N_k/A_k| < 1$.

Unfortunately, we don't know $|N_k/A_k|$. Nevertheless, to recover the unknown shift parameter ℓ, we check the positivity of the real parts of $\widetilde{B}_k/A_k$ resp. $(\widetilde{B}_k/A_k) \cdot \omega^{-kq}$ and if so conclude – possibly erroneously – that $\ell_1 = 0$ resp. $\ell_m = \ell_{m-1}$, otherwise, we put $\ell_1 = 1$ and $\ell_m = \ell_{m-1} + 2^{m-1}$, respectively. To increase the reliability of this procedure, we do this several times with noisy versions of $\boldsymbol{a}$ (!) and take the median of the ℓ-estimates. There are complexity issues why we work with noisy versions of $\boldsymbol{a}$ instead of using those of $\boldsymbol{b}$: as we know $\boldsymbol{a}$, we can perform some of the required computations with noisy versions of $\boldsymbol{a}$ in advance and this offline work will not be part of our final complexity analysis. More precisely, we produce P noisy versions $\boldsymbol{a}^1, \ldots, \boldsymbol{a}^P$ of $\boldsymbol{a}$ and calculate the Fourier coefficients $A^p_{2^m}$ (for $m \in [1, n-1]$ and $p \in [1, P]$) of these noisy versions. These $P \cdot \log N$ frequency values are stored. On input $\widetilde{\boldsymbol{b}}$, the Fourier coefficients

$\widetilde{B}_{2^m}$, $m \in [1, n-1]$, can be computed all in all with less than $2N$ additions/subtractions and less than N multiplications using parts of a classical FFT-butterfly network. For each $p \in [1, P]$ we calculate the shift estimate ℓ_p with respect to the sequence of pairs of Fourier coefficients $(A^p_{2^m}, \widetilde{B}_{2^m})_{m\in[1,n-1]}$ using the simplified version of the conditions (a) and (b). It is easy to see that the overall procedure uses less than $2N$ additions/subtractions, less than $(N+2P\cdot\log N)$ multiplications, and $P\cdot\log N$ additional storage. Finally, we take the median of $\ell_1, \ldots, \ell_P$ as the estimate of the unknown shift parameter ℓ. We call this procedure the *P-median method*.

Figure 4 shows for $N = 2^{12}$ the percentage of correct shift recovery if we use the P-median method for $P \in \{5, 11, 17\}$. The Figure shows recognition rates depending on the amount of uniform additive noise.

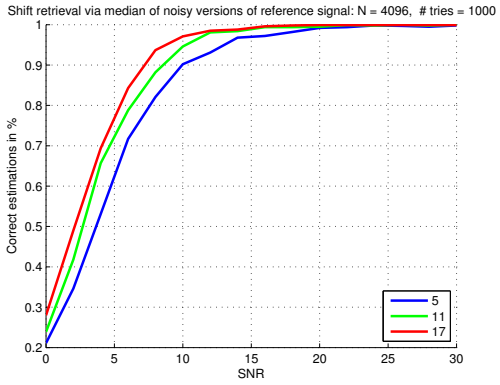

Fig. 4. Percentage of correct shift recovery for various levels of uniform additive noise.

The following table compiles the computational cost of the FFT approach with that of the P-median approach.

	# additions	# multiplications	# comparisons
FFT	$2N\log N$	$0.5N\log N - N$	N
P-median	$2N$	$N + 2P\log N$	$P\log N$

5. CONCLUSION

In this paper we have presented three contributions to compressive shift retrieval. First, we have derived a general setting for noise-free shift retrieval based on the Bézout identity. This setting allows us to simplify and extend previous approaches to shift retrieval. Based on this general setting, our second contribution is a novel method for compressive shift retrieval for scenarios where the target signal is a mixture of two differently shifted versions of a source signal. As a third contribution, we proposed a novel iterative technique for shift retrieval in noisy scenarios which is important for TDE applications. We gave a detailed analysis of the running times of the different methods and analyzed shift retrieval performance in the presence of noise.

ACKNOWLEDGMENT

The authors would like to thank four EUSIPCO reviewers for their helpful comments.

REFERENCES

[1] Yiteng Huang and Jacob Benesty, *Audio Signal Processing for Next-Generation Multimedia Communication Systems*, Kluwer, first edition, 2004.

[2] John L. Spiesberger, "Finding the right cross-correlation peak for locating sounds in multipath environments with a fourth moment function," *Journal of the Acoustical Society of America*, vol. 108, pp. 1349–1352, 2000.

[3] Takanobu Nishiura, Takeshi Yamada, Satoshi Nakamura, and Kiyohiro Shikano, "Localization of multiple sound sources based on a CSP analysis with a microphone array," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2000, pp. 1053–1056.

[4] Anantha P. Chandrakasan, Fred S. Lee, David D. Wentzloff, Vivienne Sze, Brian P. Ginsburg, Patrick P. Mercier, Denis C. Daly, and Raúl Blázquez, "Low-power impulse UWB architectures and circuits," in *Proceedings of the IEEE*, 2009, pp. 332–352.

[5] Haitham Hassanieh, Fadel Adib, Dina Katabi, and Piotr Indyk, "Faster GPS via the sparse Fourier transform," in *The 18th Annual International Conference on Mobile Computing and Networking, Mobicom'12, Istanbul, Turkey, August 22-26, 2012*, 2012, pp. 353–364.

[6] Alexandr Andoni, Piotr Indyk, Dina Katabi, and Haitham Hassanieh, "Shift finding in sub-linear time," in *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2013, New Orleans, Louisiana, USA, January 6-8, 2013*, 2013, pp. 457–465.

[7] Niels Möller, "On Schönhage's algorithm and subquadratic integer GCD computation," *Mathematics of Computation*, vol. 77, no. 261, pp. 589–607, 2008.

[8] Henrik Ohlsson, Yonina C. Eldar, Allen Y. Yang, and S. Shankar Sastry, "Compressive shift retrieval," *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4105–4113, 2014.

[9] Serge Lang, *Algebra*, vol. 211 of *Graduate Texts in Mathematics*, Springer, revised third edition, 2002.