Pattern Matching in Sub-Linear Time Using a Sparse Fourier Transform Approach

Nagaraj T. Janakiraman, Avinash Vem, Krishna R. Narayanan
Department of Electrical & Comp. Engg., Texas A&M University, College Station, TX, U.S.A
{tjnagaraj,vemavinash,krn}@tamu.edu

Abstract

We consider the problem of querying a string (or, a database) of length N bits to determine all the locations where a substring (query) of length M appears either exactly or is within a Hamming distance of K from the query. We assume that sketches of the original signal can be computed off line and stored. Using the sparse Fourier transform computation based approach introduced by Pawar and Ramchandran, we show that all such matches can be determined with high probability in sub-linear time. Specifically, if the number of matches is $L = N^{\lambda}$ and $M = N^{\mu}$, as $N \to \infty$, we show that the locations can be determined with a probability that approaches 1, with a computational complexity that is only $O\left(\max\left(\frac{N}{M}\log N, ML\log N\right)\right) = O\left(N^{\max(1-\mu,\mu+\lambda)}\log N\right)$ for $K \leq \frac{2}{3}M$. Further, the number of Fourier transform coefficients that need to be computed, stored and accessed, i.e., the sketching complexity of this algorithm is only $O\left(N^{\max(\mu,1-\mu)}\right)$. Several extensions of the main theme are also discussed.

I. Introduction and Problem Statement

We consider the pattern matching problem in the random setting which is a problem that has been studied extensively in computer science []. In this problem, we have a signal $\underline{x} := (x[1], x[2], \ldots, x[N])$ of length N symbols representing a string, library or database. We first consider the random setting of the problem in which $x[i]$'s are a sequence of independent and identically distributed (i.i.d) random variables taking values in $\mathscr{A} := \{1, -1\}$, although extensions to other alphabets $\mathscr{A} \subseteq \mathbb{R}$ are possible. We assume that a sketch of $\underline{x}$ can be computed offline and stored, and the one-time computational complexity of creating the sketch is ignored.

Exact Pattern Matching: In the exact pattern matching problem, a substring of length M of $\underline{x}$, namely $\underline{y} := \underline{x}[\tau : \tau + M - 1]$ is obtained by taking M consecutive symbols from $\underline{x}$ and is presented as a query. This pattern may appear within $\underline{x}$ in L different locations $\tau_1, \tau_2, \ldots, \tau_L$ and the objective is to determine all the locations $\tau_i, \forall i \in [1 : L]$. We consider the probabilistic version where our objective is to recover the matching locations with a probability that approaches 1 as $M, N \to \infty$.

Approximate Pattern Matching: In the approximate pattern matching version, $\underline{y}$ is a noisy version of a substring, i.e., $\underline{y} = \underline{x}[\tau : \tau + L - 1] \odot \underline{b}$ where $\underline{b}$ is a noise sequence with $b[i] \in \pm 1$ such that $d_H(\underline{y}, \underline{x}[\tau : \tau + M - 1]) \leq K$. Here d_H denotes the Hamming distance, and $\odot$ represents component-wise multiplication. The objective is to determine all locations τ_i such that $d_H(\underline{y}, \underline{x}[\tau_i : \tau_i + M - 1]) \leq K$ with a probability that approaches 1 as K, M and $N \to \infty$.

These problems are relevant to many applications including text matching, DNA sequencing, and is particularly relevant now due to the interest in applications involving huge volumes of data. The presented results are most useful in the following situations - (i) the string $\underline{x}$ is available before querying and one time computations such as computing a sketch of $\underline{x}$ can be performed off line and stored, and the complexity of computing the sketch of $\underline{x}$ can be ignored. Then, when queries in the form of $\underline{y}$ appear, one would like to decrease the computational complexity in searching for the string $\underline{y}$. (ii) The string $\underline{x}$ is not centrally available but parts of the string are sensed by different data collecting nodes distributively and communicated to a central server. A search query is presented to the server and the server needs to decide if the string appeared in the data sensed by one or more of the distributed nodes and the time instants where the query appeared. In this case, we would like to minimize the amount of data communicated by the nodes to the server and the computational complexity in searching for the string. Finally, the

This work was supported by the National Science Foundation under grants

proposed approach is most useful when the query $\underline{y}$ is not a pattern that can be predicted and, therefore, creating a look up table to quickly identify patterns is not efficient. For e.g., $\underline{x}$ is an i.i.d sequence of ± 1 and $\underline{y}$ could be a substring of $\underline{x}$.

A naive approach to searching for a substring $\underline{y}$ in $\underline{x}$ is to compute the cross correlation between $\underline{x}$ and $\underline{y}$ denoted by $\underline{r} = [r[1], \ldots, r[N]]$

$$r[m] = (\underline{x} * \underline{y})[m] \triangleq \sum_{i=1}^{M} x[m+i-1]y[i] \tag{1}$$

and choosing the index m that maximizes $r[m]$. This approach uses all the N samples of $\underline{x}$ and has a super-linear computational complexity of $MN = N^{1+\mu}$. A computationally more efficient approach uses the fact that $\underline{r}$ can be computed by taking the inverse Fourier transform of the product of the Fourier transforms of $\underline{x}$ and $\underline{y}^*[-n]$, where $\underline{y}^*[-n]$ is the conjugate of time reversed $\underline{y}$. Such an approach still uses all the N samples of $\underline{x}$ but reduces the computational complexity to $O(N \log N)$. Note that even though the Fourier transform of $\underline{x}$ can be precomputed, the N-point Fourier transform of $\underline{y}$ still needs to be computed resulting in the $O(N \log N)$ computational complexity.

Both the exact pattern matching problem and the approximate pattern matching problem have been extensively studied in computer science and two recent papers [1] and [2] provide a brief summary of the results. For the exact matching problem, Boyer and Moore presented an algorithm in [3] for finding the first occurrence of the match (only τ_1) that has an expected complexity of $O(N/M \log N) = O(N^{1-\mu} \log N)$, whereas the worst case complexity (depending on τ_1's) can be $O(N \log N)$. For large M, the algorithm indeed has an average complexity that is sub-linear in N. This algorithm has been generalized to the approximate pattern matching problem in [4] with an average case complexity of $O(NK/M \log N)$ which provides a sub-linear time algorithm only when $K \ll M$. In the work by Andoni, Hassanieh, Indyk and Katabi [1], the authors gave the first sub-linear time algorithm with a complexity of $O(N/M^{0.359})$ even for $K = O(M)$.

II. Our Main Results and Relation to Prior Work

Assuming that a sketch of $\underline{x}$ of size $O(N/M)$ can be computed and stored,

1) For the exact pattern matching problem, we present an algorithm which uses a sketching function for $\underline{y}$ with $O(\max(M \log N, N/M \log N))$ samples and a computational complexity of $O(\max(ML \log N, N/M \log N))$. When $M = N^{\mu}, L = N^{\lambda}$, this gives a sub-linear time algorithm.
2) For the approximate pattern matching problem, for $K = O(M)$, our algorithm has a sketching complexity of $\underline{y}$ is $O(\max(M \log N, N/M \log N))$ samples and computational complexity of $O(\max(ML \log N, N/M \log N))$ for all $K = O(M)$.

Our paper is inspired by and builds on two recent works by Hassanieh et al in [5] and Pawar and Ramchandran [6]. In [5], Hassanieh et al., considered the correlation function computation problem for a Global Positioning System (GPS) receiver and exploited the fact that the cross-correlation vector $\underline{r}$ is a very sparse signal in the time domain and, hence, the Fourier transform of $\underline{r}$ need not be evaluated at all the N points. In the GPS application, which was the focus of [5], the query $\underline{y}$ corresponds to the received signal from the satellites and, hence, the length of the query was at least N. As a result, the computational complexity is still $O(N \log N)$ (still linear in N) and the only the constants were improved in relation to the approach of computing the entire Fourier transform. In a later paper by Andoni *et al.,* [1], a sub-linear time algorithm for shift finding in GPS is presented; however, this algorithm is completely combinatorial and eschews algebraic techniques such as FFT-based techniques.

There are important differences between our paper and [5], [1], [3], [2]. First and foremost, the algorithms used for pattern matching are entirely different. While their algorithms are combinatorial in nature, our algorithm is algebraic and uses signal processing and coding theoretic primitives. Secondly, the system model considered in our paper is different from the model in [5], [1], [3], [2] in that we allow for preprocessing or creating a sketch of the data $\underline{x}$. Our algorithm exploits this fact and results in a computational complexity $O(N/M)$ which is better than that in [1] for the approximate pattern matching problem. Finally, we also consider the problem of finding all matches of the pattern $\underline{y}$ instead of looking for only one match. In [6], Pawar and Ramchandran present an

algorithm based on aliasing and the peeling decoder for computing the Fourier transform of a signal with noisy observations for the case when the Fourier transform is known to be sparse. This algorithm has a complexity of $O(N\log N)$ and they do not consider the pattern matching problem. Our algorithm is similar to that of Pawar and Ramchandran's algorithm with one very important distinction. We modify their algorithm to exploit the fact that the peak of the correlation function of interest is always positive. This modification is key in computing the Sparse Inverse Discrete Fourier Transform (SIDFT) with sub-linear time complexity of $O(N^{1-\alpha}\log N)$, $0<\alpha\leq 1$. Thus, one of the main contributions of this paper is to show that signal processing and coding theoretic primitives, i.e., Pawar and Ramchandran's algorithm with some modifications can be used to solve the pattern matching algorithm in sub-linear time.

III. Notations

This table below will introduce the notations we use in this paper.

Symbol	Notational Meaning
N	Size of the string or database in symbols
$M=N^{\mu}$	Length of the query in symbols
$L=N^{\lambda}$	Number of matches
K	$\max_{\tau} d_H(\underline{\mathrm{x}}[\tau:\tau+M-1],\underline{\mathrm{y}})$
$G=N^{\gamma}$	Number of blocks
$\tilde{N}=N^{1-\gamma}$	Length of one block
$A=N^{\alpha}$	Sub-sampling parameter
B	Number of shifts
d	Number of stages in the FFAST algorithm

We denote vectors using the underbar, time domain signals using lowercase letters and the frequency domain signals using uppercase letter. For example $\underline{\mathrm{x}}=(x[1],x[2],\cdots x[N])$ denotes a time domain signal with i^{th} time component denoted by $x[i]$, and $\underline{\mathrm{X}}=\mathscr{F}\underline{\mathrm{x}}$ denotes the Fourier coefficients of $\underline{\mathrm{x}}$. Matrices are denoted using uppercases letters. We differentiate a signal from a matrix by having a underbar for a signal vector. We denote the set $0,1,2\cdots,N-1$ by $[N]$.

IV. Description Of The Algorithm

In this section we describe our algorithm, with sample and time complexities that are sub-linear in N, to find the locations $\underline{\tau}=(\tau_1,\tau_2,\cdots\tau_L)$ in the string $\underline{\mathrm{x}}$, where the string (query) $\underline{\mathrm{y}}$ matches. This is achieved by computing the cross-correlation $\underline{\mathrm{r}}$ of $\underline{\mathrm{x}}$ and $\underline{\mathrm{y}}$, defined in Eqn. (1), and finding the positions where there is a significant peak.

The main idea here is that $\underline{\mathrm{R}_{XY}}$ is sparse (upto some noise) with dominant peaks at L positions (τ) where the strings match, and noise components at $N-L$ positions where the strings do not match. Consider the case of exact matching,

$$r[m] \;=\begin{cases} M, & \text{if } m\in\mathscr{T} \\ n_m, & m\in[N]-\mathscr{T} \end{cases} \tag{2}$$

where, $\mathscr{T}:=\{\tau_1,\tau_2,\cdots,\tau_L\}$, n_m is the noise component that is induced due to correlation of two i.i.d. sequence of random variables each taking values from $\mathscr{A}:=\{+1,-1\}$. The $\underline{\mathrm{r}}$ can also be computed as shown below:

$$\underline{\mathrm{r}}=\underset{\mathrm{I}}{\mathscr{F}_N^{-1}}\ \{\underset{\mathrm{II}}{\mathscr{F}_N\{\underline{\mathrm{x}}\}}\odot\ \underset{\mathrm{III}}{\mathscr{F}_N\{\underline{\mathrm{y}}'\}}\} \tag{3}$$

where $\mathscr{F}_N\{\cdot\}$ and $\mathscr{F}_N^{-1}\{\cdot\}$ refers to N-point discrete Fourier transform and its inverse respectively, $\odot$ is the point-wise multiplication operation and $y'[n]=y^*[-n]$. Fig. 1 presents a notional diagram of our Algorithm.

As evident from Equation 3, our algorithm for computing R_{XY} consists of three stages:

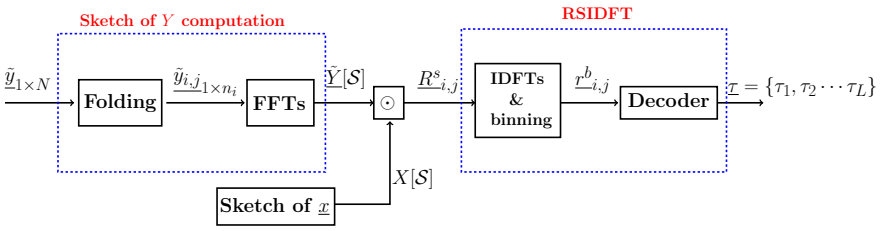

Fig. 1.

I *Computing sparse* $\mathscr{F}^{-1}$:
Since $\underline{\mathrm{r}}$ is sparse, we use a Robust Sparse Inverse Discrete Fourier Transform(RSIDFT) framework to compute the L-sparse coefficients. The architecture of RSIDFT is similar to FFAST proposed in [6], but the decoding algorithm has some key modifications to handle the noise model induced in this problem.

A. RSIDFT Framework

Let $\underline{\mathrm{R}} = \underline{\mathrm{X}} \odot \underline{\mathrm{Y}}'$ be the FFT of the cross-correlation of $\underline{\mathrm{x}}$ and $\underline{\mathrm{y}}$. We will see in Sec. IV-C how do we compute the required samples of $\underline{\mathrm{X}}$ and $\underline{\mathrm{Y}}$ but for this section we will assume that $\underline{\mathrm{X}}$ and $\underline{\mathrm{Y}}$ are available and the required samples of $\underline{\mathrm{R}}$ is computed and input to RSIDFT framework. The RSIDFT framework computes the L dominant coefficients of $\underline{\mathrm{r}}$ by using only a sub-sampled version of $\underline{\mathrm{R}}$.

Consider the RSIDFT framework shown in Figure 2. The framework consists of *d-stages*, each with a different sub-sampling factor f_i computed as following. Let $N = P_1 \times P_2 \times \cdots P_d$ be the prime factorization of N, the length of the signal $\underline{\mathrm{x}}$. For a given α, we choose distinct $f_i = \prod P_j$, $i \in [d]$ such that $f_i \approxeq N^\alpha$. In each stage, there are B *branches* with shifts from $\underline{s} = [s_1, s_2, \cdots s_B]$, where $s_1 = 0$ in the first branch and the rest chosen randomly from $[N^\alpha]$. We can also carefully choose the shifts to satisfy mutual coherence property and restricted isometric property described in the analysis section.

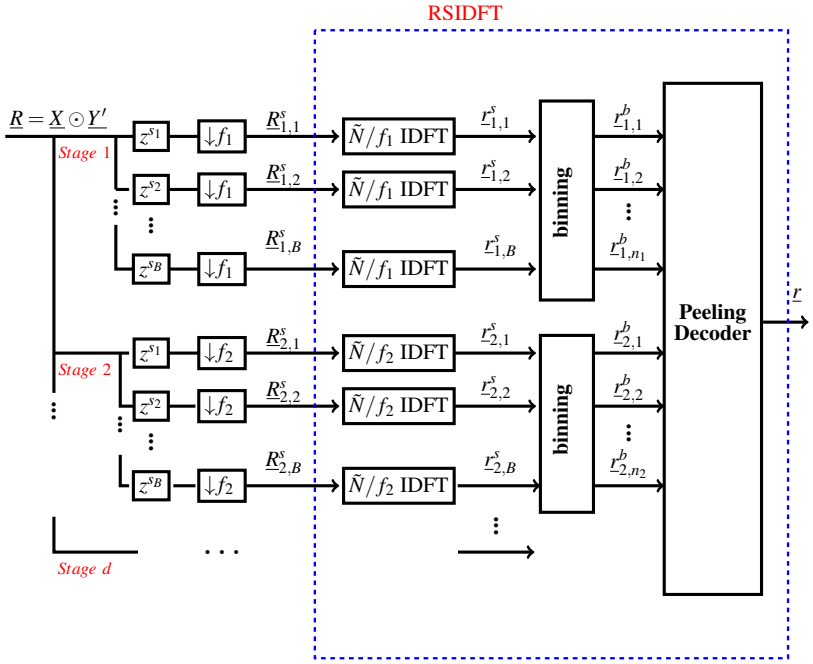

Fig. 2. RSIDFT Framework to compute inverse Fourier Transform of a signal $\underline{\mathrm{R}}$ that is sparse in time domain.

Given the input $\underline{\mathrm{R}}$, in branch j of i^{th} stage or referred to as *branch* (i,j) for convenience, RSIDFT sub-samples the signal $\underline{\mathrm{R}}$ at

$$\mathscr{S}_{i,j} := \{s_j,\ s_j+f_i,\ s_j+2f_i,\ \cdots s_j+n_i f_i\}, \tag{4}$$

where $n_i := \frac{N}{f_i}$ to obtain $\underline{\mathrm{R}}^s_{i,j} = \underline{\mathrm{R}}[\mathscr{S}_{i,j}]$. The sub-sampling operation is followed by a n_i-point IDFT in each branch of stage i to obtain $\underline{\mathrm{r}}^s_{i,j}$. Notice that $\underline{\mathrm{r}}^s_{i,j}$ is an aliased version of $\underline{\mathrm{r}}$ due to the property that sub-sampling in Fourier domain is equivalent to aliasing in time domain.

Let $\underline{\mathrm{r}}^b_{i,k}$ be the vector of observations that is formed by combining all k^{th} coefficients of $\underline{\mathrm{r}}^s_{i,k}$ (belonging to stage i) together as a vector, where $k \in [0 : n_i - 1]$, i.e.

$$\underline{\mathrm{r}}^b_{i,k} = \begin{bmatrix} r^s_{i,1}[k] \\ r^s_{i,2}[k] \\ \vdots \\ r^s_{i,B}[k] \end{bmatrix}$$

More formally we can write the relationship between the the observation vectors $\underline{\mathrm{r}}^b_{i,j}$ at bin (i,j) and sparse vector to be estimated $\underline{\mathrm{r}}$ as:

$$\underline{\mathrm{r}}^b_{i,k} = \left[\underline{w}^k, \underline{w}^{k+n_i}, \ldots, \underline{w}^{k+(f_i-1)n_i}\right] \begin{bmatrix} r[k+(0)n_i] \\ r[k+(1)n_i] \\ \vdots \\ r[k+(f_i-1)n_i] \end{bmatrix} \qquad \text{where } \underline{w}^k = \begin{bmatrix} e^{\frac{j2\pi k s_1}{N}} \\ e^{\frac{j2\pi k s_2}{N}} \\ \vdots \\ e^{\frac{j2\pi k s_B}{N}} \end{bmatrix} \tag{5}$$

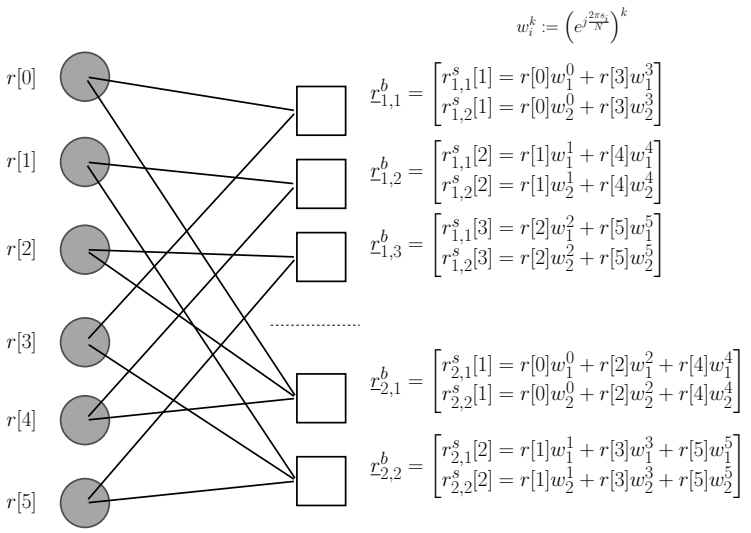

Fig. 3. Example of a Tanner graph formed in a RSIDFT framework with system parameters being $d = 2$, $B = 2$, $N = 6$, $f_1 = 2$ and $f_2 = 3$. The variable nodes (colored gray circles) represent the cross-correlation vector $\underline{\mathrm{r}}$ and the bin nodes (uncolored white boxes) represent the binned observation vector $\underline{\mathrm{r}}^b_{i,k}$. The figure also illustrates the relationship between $\underline{\mathrm{r}}^b_{i,k}$ and $\underline{\mathrm{r}}$.

In Fig. 3 we represent the relation between $\underline{\mathrm{r}}$ and $\tilde{\underline{\mathrm{r}}}^b := [\underline{\mathrm{r}}^b_{1,1}, \underline{\mathrm{r}}^b_{1,2}, \ldots, \underline{\mathrm{r}}^b_{1,n_1}, \ldots, \underline{\mathrm{r}}^b_{2,1}, \ldots, \underline{\mathrm{r}}^b_{2,n_2}, \ldots, \underline{\mathrm{r}}^b_{B,1}, \ldots, \underline{\mathrm{r}}^b_{B,n_B}]$ via an example using Tanner graph. We refer to $\tilde{\underline{\mathrm{r}}}^b$ as sensing signal. The nodes on the left, which we refer to as *variable nodes*, represent the N elements of vector $\underline{\mathrm{r}}$. And similarly the nodes on the right, which we refer to as *bin nodes*, represent the $\sum_{i \le B} n_i$ sub-sensing signals. We will now describe the decoding algorithm which takes the sensing signal $\tilde{\underline{\mathrm{r}}}^b$ as input and estimates the L-sparse $\underline{\mathrm{r}}$.

B. Decoder

Observe from the Tanner graph that the degree of each bit node is d and that of each bin node is approximately N^{α}. We refer to a bin node as *zero-ton* (or $\mathcal{H}_z$) if the number of variable nodes with significant amplitude connected to the bin node is zero. The *singleton ($\mathcal{H}_s$), double-ton ($\mathcal{H}_d$) and multi-ton ($\mathcal{H}_m$)* bin nodes are defined similarly where the number of significant variable nodes connected are one, two and greater than two, respectively. The peeling decoder has the following three steps in the decoding process.

1) Bin Classification: In this step a bin node is classified as a zero-ton or a singleton or a multi-ton. At bin (i,j) the classification is done based on comparing the first observation $r^b_{i,j}[1]$, which corresponds to zero shift, with a predefined threshold. Let the value of $r^b_{i,j}[1]$ be z, then the classification rules can be written as follows:

$$\widehat{\mathcal{H}}_{i,j} = \begin{cases} \mathcal{H}_z & z/M < \gamma_1 \\ \mathcal{H}_s & \gamma_1 < z/M < \gamma_2 \\ \mathcal{H}_d & \gamma_2 < z/M < \gamma_3 \\ \mathcal{H}_m & z/M > \gamma_3 \end{cases} \tag{6}$$

where $(\gamma_1,\gamma_2,\gamma_3) = (\frac{1-2\eta}{2}, \frac{3-4\eta}{2}, \frac{5-6\eta}{2})$. Note that for the case of exact matching $\eta = 0$.
2) Singleton decoding: If a bin node (i,j) is classified as a singleton, we need to identify the position of the significant non-zero variable node connected to it. This is done by correlating the observation vector $\underline{\mathrm{r}}^b_{i,j}$ with each column of $\mathbf{W}_{i,j} := [\underline{w}^j, \underline{w}^{j+n_i}, \ldots, \underline{w}^{j+(f_i-1)n_i}]$ and choose the index that maximizes the correlation value.

$$\hat{k} = \underset{k \in \{j+ln_i\}}{\arg\max}\ \underline{w}^k\ \underline{\mathrm{r}}^b_{i,j}$$

The value of the variable node connected to the singleton bin is estimated as follows:

$$\hat{r}[\hat{k}] = M(1-\eta).$$

Note that for the case of exact matching we know the value to be exactly equal to M which is our estimate in the case of exact matching ($\eta = 0$). But in the case of approximate matching the actual value of $x[k] \in \{M(1-2\eta), \ldots, M-1, M\}$ and our estimate $\hat{r}[\hat{k}] = M(1-\eta)$, the mid-point of the range, is only a loose approximate, this would suffice for our purposes as we are mainly interested in recovering only the positions of matches i.e. the indices of the sparse coefficients in $\underline{\mathrm{r}}$ nit their values.

3) Peeling Process: The main idea behind the peeling based decoder is to find a singleton bin, identify the significant variable node connected to the bin, decode it's value and remove it's contribution from all the bin nodes connected to that variable node. Although the main idea is similar for exact matching and the approximate matching scenarios, there are some subtle differences in their implementation.

Exact Matching: In the case of exact matching, we remove the decoded variable node's contribution from all the bin nodes it is connected to.
Approximate Matching: In this case we remove the decoded variable node's contribution only from singleton and double-ton bins and do not alter the bins which are classified to be multi-tons with degree more than two.

We present the overall recovery algorithm, which comprises of *bin classification, singleton decoding* and *peeling process*, in the Algorithm 1 pseudo-code.

C. Sketches of $\underline{\mathrm{X}}$ and $\underline{\mathrm{Y}}$

As we have already seen in Sec. IV-A the RSDIFT framework requires the values of $\underline{\mathrm{R}}(= \underline{\mathrm{X}} \odot \underline{\mathrm{Y}})$ only at indices $\mathscr{S}$ or in other words we need $\underline{\mathrm{X}}$ and $\underline{\mathrm{Y}}$ only at the indices $\mathscr{S}$.

Algorithm 1 Peeling based recovery algorithm

Compute $\widehat{\mathcal{H}}_{i,j}$ for $i \in [B], j \in [n_i]$. See Eqn. (6)

while $\exists\ i,j : \widehat{\mathcal{H}}_{i,j} = \mathcal{H}_s$, **do**

$(\hat{k}, \hat{r}[\hat{k}])$ =**Singleton-Decoder**$(\underline{\mathrm{r}}^b_{i,j})$

Assign $\hat{r}[\hat{k}]$ to $\hat{k}^{\text{th}}$ variable in bin (i,j)

for $(i_0, j_0) \in \mathcal{N}(\hat{k})$ **do**

$\underline{\mathrm{r}}^b_{i_0,j_0} \leftarrow \underline{\mathrm{r}}^b_{i_0,j_0} - \hat{r}[\hat{k}]\mathbf{g}_{\hat{k}}$ *Exact Matching*

$\underline{\mathrm{r}}^b_{i_0,j_0} \leftarrow \underline{\mathrm{r}}^b_{i_0,j_0} - \hat{r}[\hat{k}]\mathbf{g}_{\hat{k}}$ only if $\widehat{\mathcal{H}}_{i_0,j_0} = \mathcal{H}_s$ or $\mathcal{H}_d$ *Approximate Matching*

Recompute $\widehat{\mathcal{H}}_{i_0,j_0}$

Algorithm 2 Singleton-Decoder

Input: $\underline{\mathrm{r}}^b_{i,j}$

Output: $(\hat{k}, \hat{r}[\hat{k}])$

Estimate singleton index to be $\hat{k} = \underset{k \in \{j+ln_i\}}{\arg\max}\ \underline{w}^k\ \underline{\mathrm{r}}^b_{i,j}$

Estimate the value to be:

$$\hat{r}[\hat{k}] = \begin{cases} M & \text{Exact Matching case} \\ \frac{M-K}{2} & \text{Approximate Matching case} \end{cases}$$

Computing the sketch of $\underline{\mathrm{x}}$: We assume that the sketch of $\underline{\mathrm{x}}$, $\underline{\mathrm{X}}[\mathscr{S}] = \{X[i], i \in \mathscr{S}\}$ is pre-computed and stored in a database.

Computing the sketch of $\underline{\mathrm{y}}$: For every new query $\underline{\mathrm{y}}$, only $\{\underline{\mathrm{Y}}'[\mathscr{S}_{i,j}], i \in [d], j \in [B]\}$ needs to be computed where the subsets $\mathscr{S}_{i,j}$ are defined in Eq. (4). Naively, the FFT algorithm can be used to compute $\underline{\mathrm{Y}}'$ and the required subset of coefficients can be taken but this would be of $O(N \log N)$ complexity. We observe that $\underline{\mathrm{Y}}'[\mathscr{S}_{i,j}]$ is $\underline{\mathrm{Y}}'$ shifted by s_j and sub-sampled by a factor of f_i. Thus for a given (i,j) this corresponds to, in time domain, a point-wise multiplication by $[1, W_{s_j}, W_{s_j}^2, \ldots, W_{s_j}^{N-1}]$ followed by *folding* the signal into f_i number of length $\frac{N}{f_i}$ signals and adding them up resulting in a single length $\frac{N}{f_i}$ signal denoted by $\underline{\mathrm{y}}'_{i,j}$. Formally the *folding* operation can be described as follows:

$$\underline{\mathrm{y}}'_{i,j} = \sum_{m=0}^{f_i-1} \underline{\mathrm{y}}'[mn_i : (m+1)n_i - 1] \odot [W_{s_j}^{mn_i}, W_{s_j}^{mn_i+1}, \ldots, W_{s_j}^{(m+1)n_i-1}], \qquad W_{s_j} = e^{\frac{j2\pi s_j}{N}} \tag{7}$$

where $n_i = \frac{N}{f_i}$. Taking n_i-point DFT of $\underline{\mathrm{y}}'_{i,j}$ produces $\underline{\mathrm{Y}}'[\mathscr{S}_{i,j}]$ i.e. $\underline{\mathrm{Y}}'$ sampled only at $\mathscr{S}_{i,j}$ indices which is what we need in branch (i,j). To obtain all the samples in $\mathscr{S}$ required for the RSDIFT framework, the *folding* technique needs to be carried out for each (i,j), for $i \in [d], j \in [B]$, a total of $\approx dB\ \ N^{1-\alpha}$-point DFTs.

V. Performance Analysis

In this section, we will analyze the overall probability of error involved in finding the correct position of match. This can be done by analyzing the following three error events independently and then using a union bound to bound the total probability of error.

- $\mathscr{E}_1$-*Bin Classification*: Event that a bin is wrongly classified
- $\mathscr{E}_2$-*Position Identification*: Event that a position is wrongly identified given the bin is correctly identified as a singleton
- $\mathscr{E}_3$-*Peeling Process* : Event that the peeling process fails to recover the L significant correlation coefficients

A. Bin Classification

Lemma 1. *The probability of bin classification error at any bin (i,j) can be upper bounded by*

$$\mathbb{P}[\mathscr{E}_1] \leq 6e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}}$$

Proof.

$$\begin{aligned}
\mathbb{P}[\mathscr{E}_1] &= \mathbb{P}[\mathcal{H}_z]\mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_z] \;+\; \mathbb{P}[\mathcal{H}_s]\mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_s] \;+\; \mathbb{P}[\mathcal{H}_d]\mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_d\cup\mathcal{H}_m] \\
&\leq \mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_z] \;+\; \mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_s] \;+\; \mathbb{P}[\mathscr{E}_1|\widehat{\mathcal{H}}_{i,j}=\mathcal{H}_d\cup\mathcal{H}_m] \\
&\leq e^{-\frac{N^{\mu-\alpha}(1-2\eta)^2}{8}} + 2e^{-\frac{N^{\mu-\alpha}(1-4\eta)^2}{16}} + 2e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}} + e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}} \\
&\leq 6e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}}
\end{aligned}$$

where the inequalities in the third line are due to Lemmas 7, 8, 9 and 10 respectively. □

B. Position Identification

We will analyze the singleton identification in two separate cases:

- $\mathscr{E}_{21}$: Event where the position is identified incorrectly when the bin is classified correctly a singleton
- $\mathscr{E}_{22}$: In the case of approximate matching, event where the position is identified incorrectly when the bin is originally a double-ton and one of the non-zero variable nodes has already been peeled off

Lemma 2. *For the choice of $B = 4c_1^2 \log 5N$, the probability of error in identifying the position of a singleton at any bin (i,j) can be upper bounded by*

$$\mathbb{P}[\mathscr{E}_{21}] \leq \exp\left\{-\frac{N^{\mu-\alpha}(1-2\eta)^2(c_1^2-1)}{8(c_1^2+1)}\right\}$$

Lemma 3. *The probability of error in identifying the position of the second non-zero variable node at a double-ton at any bin (i,j) can be upper bounded by*

$$\mathbb{P}[\mathscr{E}_{22}] \leq \ldots$$

$\mathscr{E}_{21}$**:**

$$\begin{aligned}
\underline{z}_{i,j} &= \left[\underline{\mathrm{w}}_{j_1}, \underline{\mathrm{w}}_{j_2}, \quad \cdots \quad \underline{\mathrm{w}}_{j_p}, \quad \cdots \quad \underline{\mathrm{w}}_{j_{f_i}}\right] \times \begin{bmatrix} n_1 \\ \vdots \\ r[j_p] \\ \vdots \\ n_j \\ \vdots \\ n_{f_i} \end{bmatrix} \\
&= r[j_p]\ \underline{\mathrm{w}}_{j_p} + \sum_{k\neq p} n_k \underline{\mathrm{w}}_{j_k}
\end{aligned}$$

where for convenience we use a simpler notation $j_k = j + (k-1)\frac{N}{f_i}, \underline{\mathrm{w}}_{j_k} = \underline{\mathrm{w}}^{j_k}$ as defined in Eq. and $n_l = \sum_{k=0}^{M-1} x[\theta_\ell + k]y[k]$ as defined in Eq. (9).

The estimated position $\hat{p}$ is given by

$$\hat{p} = \arg\max_{l} \quad \frac{\underline{\mathrm{w}}_{j_l}^{\dagger} \underline{z}_{i,j}}{B} \tag{8}$$

where $\dagger$ denotes the conjugate transpose of the vector. Also note that $||\underline{\mathrm{w}}_{j_k}|| = B$ for any j and k. From Eq. (8) we observe that the position is wrongly identified when $\exists p'$ such that

$$r[j_p] + \frac{1}{B}\sum_{k\neq p} n_k \underline{\mathrm{w}}_{j_p}^{\dagger}\underline{\mathrm{w}}_{j_k} \leq \frac{r[j_p]}{B}\ \underline{\mathrm{w}}_{j_{p'}}^{\dagger}\underline{\mathrm{w}}_{j_p} + n_{p'} + \frac{1}{B}\sum_{k\neq p,p'} n_k \underline{\mathrm{w}}_{j_{p'}}^{\dagger}\underline{\mathrm{w}}_{j_k}$$

$$\leftrightarrow \sum_{k\neq p,p'} \alpha_k n_k + \beta_k n_{p'} \geq r[j_p]\left(1 - \frac{\underline{\mathrm{w}}_{j_{p'}}^{\dagger}\underline{\mathrm{w}}_{j_p}}{B}\right) \geq M(1-2\eta)(1-\mu_{\max})$$

where α_k and β are constants and can be shown to be in the range $\alpha_k \in [-2\mu_{\max}, 2\mu_{\max}]$ and $\beta \in [1-\mu_{\max}, 1+\mu_{\max}]$. Now using the bound given Chernoff Lemma in Lem. 5 we obtain

$$\begin{aligned}
\mathbb{P}[\mathscr{E}_{21}] &\leq \exp\left\{-\frac{2M(1-2\eta)^2(1-\mu_{\max})^2}{16 f_i \mu_{\max}^2 + 4(1+\mu_{\max})^2}\right\} \\
&\leq \exp\left\{-\frac{2M(1-2\eta)^2(1-\mu_{\max})^2}{16(f_i\mu_{\max}^2+1)}\right\} \\
&\leq \exp\left\{-\frac{2M(1-2\eta)^2(c_1-1)^2}{16(f_i+c_1^2)}\right\} \\
&\approx \exp\left\{-\frac{N^{\mu-\alpha}(1-2\eta)^2(c_1^2-1)}{8(c_1^2+1)}\right\}
\end{aligned}$$

where for the choice of $B = 4c_1^2 \log 5N$, $\mu_{\max} \leq 2\sqrt{\frac{\log 5N}{B}} \leq 1/c_1$.

Approximate Matching:

$$\mathbf{Z_i} = \begin{bmatrix}\mathbf{s_1} & \cdots & \mathbf{s_p} & \cdots & \mathbf{s_A}\end{bmatrix} \times \begin{bmatrix} n_1 \\ \vdots \\ R_{XY}[p] \\ \vdots \\ n_j \\ \vdots \\ n_A \end{bmatrix}$$

where $n_j \sim \mathscr{N}(0, M),\ j \neq p$.

$$\begin{aligned} Z_i[1] &= R_{XY}[p] + \textstyle\sum_{j\neq p} n_j \\ &= R_{XY}[p] + n \end{aligned}$$

where $n \sim \mathscr{N}(0, (N^{\alpha}-1)M)$. Once we identify a Singleton with probability of error $Pe_s \leq 2e^{-\frac{(1-2\eta)^2 N^{\mu-\alpha}}{8}}$, we can fix the value of $R_{XY}[p] = M(1-\eta/2)$ since we are only interested in finding the positions and not the exact value of correlations.

Now that we know $R_{XY}[p]$,

$$\mathbf{Z_i} \ = \ R_{XY}[p]\ \mathbf{s_p} + \sum_{j\neq p} n_j \mathbf{s_j}$$

Also, let p_1 be the position of the previously peeled node from this check-node. There can only be at most one peeled edge as we restrict our peeling process to a doubleton and do not consider other multi-tons.

Let us consider two cases:

Case 1: $p' = p$

$$\begin{aligned} c_1 &= \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{Z_i} \ = \ R_{XY}[p]\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_p} \ + \ \textstyle\sum_{j\neq p,p_1} n_j\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_j} \ \pm \ \frac{\eta M}{2}\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_{p_1}} \\ &\leq B\ (M-\eta M/2) + \textstyle\sum_{j\neq p} 2n_j\ \mu_{max} \pm \frac{\eta M}{2}\mu_{max} \end{aligned}$$

Case 2: $p' \neq p$

$$\begin{aligned} c_2 &= \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{Z_i} \ = \ R_{XY}[p]\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_p} + \textstyle\sum_{j\neq p',p,p_1} n_j\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_j} \ + \ n_{p'}\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_p} \ \pm \ \frac{\eta M}{2}\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_{p_1}} \\ &\leq (M-\eta M/2)\ \mu_{max} + \textstyle\sum_{j\neq p',p}\ 2n_j\ \mu_{max} \ + \ n_{p'}B \pm \frac{\eta M}{2}\mu_{max} \end{aligned}$$

$$\begin{aligned} c_1 - c_2 &= R_{XY}[p](B - \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_p}) \ - \ n_{p'}(B - \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s}'_{\mathbf{p}}) \ + \ \textstyle\sum_{j\neq p',p,p_1} n_j(\ \mathbf{s}_{\mathbf{p}}^{\mathbf{T}}\ \mathbf{s_j} - \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_j}) \pm \ \eta M\ \mathbf{s}_{\mathbf{p}'}^{\mathbf{T}}\ \mathbf{s_{p_1}} \\ &\leq (M-\eta M/2)(B-\mu_{max}) \ - \ n_{p'}(B-\mu_{max}) \ + \ \textstyle\sum_{j\neq p',p} n_j\mu_{max} \pm \eta M\mu_{max} \end{aligned}$$

Notice that c_1 and c_2 are both Gaussian random variables given by

$$\begin{aligned} c_1 &\sim \mathscr{N}(B\ (M-\eta M/2) \pm \tfrac{\eta M}{2}\mu_{max}\ ,\ 4N^{\alpha}MB\log(5N)) \\ c_2 &\sim \mathscr{N}(2M\sqrt{B\log(5N)}\ ,\ M\ B^2 + 4N^{\alpha}MB\log(5N)) \\ c_1 - c_2 &\sim \mathscr{N}((M-\eta M/2)(B-\mu_{max}) \pm \eta M\mu_{max}\ ,\ M((B-\mu_{max})^2 + (N^{\alpha}-2)\mu_{max}^2) \end{aligned}$$

The probability that event $\mathscr{E}_2$ happens, given that $\bar{\mathscr{E}_1}$ doesn't happen is given by

$$P(\mathscr{E}_2/\bar{\mathscr{E}_1}) = Pr(c_2 > c_1)$$

$$P(\mathscr{E}_2/\bar{\mathscr{E}_1}) \leq Q\left(\sqrt{\frac{((M-\eta M/2)(B-\mu_{max}) \pm \eta M\mu_{max})^2}{M(B-\mu_{max})^2 + M(N^{\alpha}-2)\mu_{max}^2)}}\right)$$

where $\mu_{max} = 2\sqrt{B\log 5N^{\alpha}}$. If $B = O(\log 5N^{\alpha})$, then the above equation reduces to

$$P(\mathscr{E}_2/\bar{\mathscr{E}_1}) \leq Q\left(\sqrt{\frac{M(1-3\eta/2)^2}{1+4\ (N^{\alpha}-2)}}\right)$$

If $\mu > \alpha$, the error vanishes.

VI. Complexity Analysis

In this section, we will analyze the number of samples used from the actual database to run the algorithm and also the computational complexity as a function of the system parameters.

A. Sample Complexity

As stated in the problem statement, we exploit the sparseness in IDFT computations to compute the correlations using less number of samples from the database.

In each branch of the FFAST algorithm, executed over a block of samples, we down-sample the $\tilde{N}$ samples by a factor of N^{α} to get $N^{1-\gamma-\alpha}$ samples. We also do this for each chosen shift and we get a total of $N^{1-\gamma-\alpha+\beta}$ samples per block per stage. We repeat this for $d = \frac{1-\gamma}{\alpha}$ such stages to get a total complexity of $dN^{1-\gamma-\alpha+\beta}$ samples per block. So, the total number of samples is given by

$$\text{Total \# of samples required (S)} \ = \ \underbrace{\frac{1-\gamma}{\alpha}}_{d \text{ stages}}\ \underbrace{N^{1-\gamma-\alpha+\beta}}_{\text{Samples per block per stage}}\ \underbrace{N^{\gamma}}_{\text{\# of blocks}} \ = \ \frac{1-\gamma}{\alpha}\ N^{1-\alpha+\beta}$$

B. Computational Complexity

Consider the operations involved in the computation of correlation of X and Y, R_{XY}, as shown below.

$$R_{XY} = \underbrace{IDFT}_{\text{I}} \{\underbrace{DFT\{X\}}_{\text{II}} \times \underbrace{DFT\{Y\}}_{\text{III}}\}$$

In each block of samples from the database, the process of computing the correlation involves three sets of operations: two $\tilde{N}$-point DFT operations (II, III) sampled at $N^{1-\gamma-\alpha+\beta}$ points(based on sampling requirements of FFAST architecture) and one sparse-IDFFT operation (I). We assume that the database already contains sampled version of DFT $\{ X \}$ stored and hence we exclude those computations from the complexity calculations. So, it is enough that we analyze the computations involved in operations (I, III) on each block to get the overall computational complexity.

1) Operation - III:
Notice that the operation $DFT\{Y\}$ is just a one time computation and can be reused in each block since the query is same for all blocks. Since we only need to compute the sampled version of the DFT$\{Y\}$ in each branch, we can do some clever implementations to reduce the complexity. We can create aliasing on Y and then take a shorter length ($N^{1-\gamma-\alpha}$-point) DFT to obtain the sampled version of $\tilde{N}$-point DFT of Y.
This method of computing sampled DFT$\{Y\}$ involves two operations - folding and adding (aliasing), and then a $N^{1-\gamma-\alpha}$-point DFT. The complexity involved in computing down-sampled DFT$\{Y\}$, C_{III}, is given by

$$C_{III} = \underbrace{\frac{1-\gamma}{\alpha}}_{d \text{ stages}} \Big(\underbrace{N^{\delta+\beta}}_{\text{\# of additions (aliasing)}} + \underbrace{N^{1-\gamma-\alpha+\beta} \log N^{1-\gamma-\alpha}}_{\text{Shorter FFTs}} \Big)$$

Folding and adding, for each shift, involves adding N^{α} vectors of length $N^{1-\gamma-\alpha}$. We know that the length of the query is $L = N^{\delta}$, i.e., the number of non-zero elements in Y (zero-padded version of the query) is L and hence we only need to compute L additions instead of the length of the vector.

2) Operation - I:
Taking advantage of the fact that the correlations are sparse (with some noise), we use a FFAST based architecture to reduce the complexity involved in computing IDFT. The number of computations involved in this process,C_I, is given by

$$C_I = \underbrace{N^{\gamma}}_{\text{\# of blocks}} \underbrace{\frac{1-\gamma}{\alpha}}_{d \text{ stages}} \underbrace{N^{1-\gamma-\alpha+\beta} \log N^{1-\gamma-\alpha}}_{\text{Shorter IFFTs /block/stage}} = \frac{1-\gamma}{\alpha} N^{1-\alpha+\beta} \log N^{1-\gamma-\alpha}$$

Total number of computations, $C = C_{III} + C_I$, is given by

$$C = \frac{1-\gamma}{\alpha} (N^{\delta+\beta} + N^{1-\gamma-\alpha+\beta} \log N^{1-\gamma-\alpha} + N^{1-\alpha+\beta} \log N^{1-\gamma-\alpha})$$

Lemma 4 (Chernoff Bound for bounded random variables)**.** *Let $X_1, X_2, \ldots, X_n$ be a sequence of independent random variables such that $X_i \in \{-1, +1\}$ for all i and $E[X_i] = \mu$ for all i. Then for any $\delta > 0$:*

$$\textbf{\textit{Upper Tail}} : \mathbb{P}\left[\frac{1}{n}\sum (X_i - \mu) \geq \delta\right] \leq e^{-\frac{n\delta^2}{2}}$$

$$\textbf{\textit{Lower Tail}} : \mathbb{P}\left[\frac{1}{n}\sum (X_i - \mu) \leq -\delta\right] \leq e^{-\frac{n\delta^2}{4}}$$

Lemma 5 (Variant of Hoeffding Bound)**.** *Let $X_1, X_2, \ldots, X_n$ be a sequence of independent random variables such that $X_i \in [a_i, b_i]$ and $E[X_i] = \mu$ for all i. Then for any $\delta > 0$:*

$$\textbf{\textit{Upper Tail}} : \mathbb{P}\left[\sum (X_i - \mu) \geq \delta\right] \leq \exp\left\{-\frac{2\delta^2}{\sum (b_i - a_i)^2}\right\}$$

Remark 6. *Let us consider $r[\theta_1],\ldots,r[\theta_{f_i}]$ where $\theta_i \notin \{\tau_1,\ldots,\tau_L\}$ are not one of the matching positions. Then we can show that $\mathbb{P}[x[\theta_i+k]y[k]=+1]$ with probability 1/2 and $\mathbb{E}[x[\theta_i+k]y[k]]=0$. We also need to show that the set of random variables $\{x[\theta_i+k]y[k] : i \in \{1,2,\ldots f_i\}, k \in [M]\}$ are independent. I was able to show this for the case of $M=3$. I don't see a simple way of extending this to the case of general M.*

APPENDIX A
BIN CLASSIFICATION ERRORS

We employ classification rules based only on the first element of the measurement vector at bin (i,j) which can be given by

$$Z[1] = \begin{cases} \sum_{\ell=0}^{f_i-1}\sum_{k=0}^{M-1} n_{l,k} & \text{if} \quad \mathcal{H}=\mathcal{H}_z \\ M_1 + \sum_{\ell=0}^{f_i-2}\sum_{k=0}^{M-1} n_{l,k} & \text{if} \quad \mathcal{H}=\mathcal{H}_s \\ M_1+M_2+\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} & \text{if} \quad \mathcal{H}=\mathcal{H}_d \end{cases} \tag{9}$$

where $n_{l,k} = x[\theta_\ell+k]y[k]$ and $\theta_\ell \notin \{\tau_1,\tau_2,\ldots,\tau_L\}$. Also for the case of exact matching $M_1=M_2=M$ whereas in the case of approximate matching the values of $M_1,M_2 \in [M(1-2\eta):M]$.

Lemma 7 (zero-ton)**.** *Given that the bin (i,j) is a zero-ton, the classification error can be bounded by*

$$\mathbb{P}[\mathscr{E}_1|\mathcal{H}_z] \le e^{-\frac{N^{\mu-\alpha}(1-2\eta)^2}{8}}$$

Proof. The above expression can be derived by observing that a bin is not classified as zero-ton if $\frac{Z[1]}{M} \ge \frac{1-2\eta}{2}$. Let us denote the probability of this event as p_{z1} which can be bounded as:

$$\begin{aligned} p_{z1} =& \mathbb{P}\left[\frac{Z[1]}{Mf_i} \ge \frac{1-2\eta}{2f_i}\right] \\ &\le e^{-\frac{Mf_i(1-2\eta)^2}{8f_i^2}} \\ &\approx e^{-\frac{N^{\mu-\alpha}(1-2\eta)^2}{8}} \end{aligned}$$

where the second bound is due to Eqn. (9) and Lemma. 4. The approximation in the third line is from our design that all the f_i are chosen such that $f_i \approx N^\alpha$ and $M=N^\mu$. □

Lemma 8 (singleton)**.** *Given that the bin (i,j) is a singleton, the classification error can be bounded by*

$$\mathbb{P}[\mathscr{E}_1|\mathcal{H}_s] \le 2e^{-\frac{N^{\mu-\alpha}(1-4\eta)^2}{16}}$$

Proof. We observe that a bin is not classified as singleton if $\frac{Z[1]}{M} \le \frac{1-2\eta}{2}$ or $\frac{Z[1]}{M} \ge \frac{3-4\eta}{2}$. Let us denote the probability of the two events as p_{s1} and p_{s2} respectively which can be bounded as:

$$\begin{aligned} p_{s1} &= \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-2}\sum_{k=0}^{M-1} n_{l,k} \le \frac{1-2\eta}{2} - \frac{M_1}{M}\right] \\ &\le \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-2}\sum_{k=0}^{M-1} n_{l,k} \le -\frac{1-2\eta}{2}\right] \\ &\le e^{-\frac{Mf_i(1-2\eta)^2}{16f_i^2}} \\ &\approx e^{-\frac{N^{\mu-\alpha}(1-2\eta)^2}{16}} \end{aligned}$$

where we used *lower tail* of Lemma 4 and $f_i \approx N^{\alpha}$ and the lower bound on $\frac{M_1}{M} \geq (1-2\eta)$. Similarly p_{s2} can be upper bounded by:

$$\begin{aligned} p_{s2} &= \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-2}\sum_{k=0}^{M-1} n_{l,k} \geq \frac{3-4\eta}{2} - \frac{M_1}{M}\right] \\ &\leq \mathbb{P}\left[\frac{1}{Mf_i}\sum_{\ell=0}^{f_i-2}\sum_{k=0}^{M-1} n_{l,k} \geq -\frac{1-4\eta}{2f_i}\right] \\ &\approx e^{-\frac{N^{\mu-\alpha}(1-4\eta)^2}{8}} \end{aligned}$$

Thus the overall probability of error for classifying a singleton can be obtained by combining p_{s1} and p_{s2}. □

Lemma 9 (double-ton)**.** *Given that the bin (i,j) is a double-ton, the classification error can be bounded by*

$$\mathbb{P}[\mathscr{E}_1|\mathcal{H}_d] \leq 2e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}}$$

Proof. We observe that a bin is not classified as double-ton if $\frac{Z[1]}{M} \leq \frac{3-4\eta}{2}$ or $\frac{Z[1]}{M} \geq \frac{5-6\eta}{2}$. Let us denote the probability of these two events as p_{d1} and p_{d2} respectively which can be bounded similar to Lemma 8.

$$\begin{aligned} p_{d1} &= \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} \leq \frac{3-4\eta}{2} - \frac{M_1+M_2}{M}\right] \\ &\leq \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} \leq -\frac{1-4\eta}{2}\right] \\ &\leq e^{-\frac{M(f_i-2)(1-4\eta)^2}{16(f_i-2)^2}} \\ &\approx e^{-\frac{N^{\mu-\alpha}(1-4\eta)^2}{16}}. \end{aligned}$$

Similarly p_{d2} can be bounded as

$$\begin{aligned} p_{d2} &= \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} \geq \frac{5-6\eta}{2} - \frac{M_1+M_2}{M}\right] \\ &\leq \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} \geq \frac{1-6\eta}{2}\right] \\ &\leq e^{-\frac{M(f_i-2)(1-6\eta)^2}{8(f_i-2)^2}} \\ &\approx e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{8}} \end{aligned}$$

where we use the lower bounds $M_1, M_2 \leq M$. □

Lemma 10 (multi-ton)**.** *Given that the bin (i,j) is a multi-ton, the classification error can be bounded by*

$$\mathbb{P}[\mathscr{E}_1|\mathcal{H}_m] \leq e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}}$$

Proof. We observe that a bin is not classified as multi-ton if $\frac{Z[1]}{M} \leq \frac{5-6\eta}{2}$. Let us denote the probability of this event as p_{m1} which can be bounded as:

$$\begin{aligned}
p_{m1} &= \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-3}\sum_{k=0}^{M-1} n_{l,k} \leq \frac{5-6\eta}{2} - \frac{M_m}{M}\right] \\
&\leq \mathbb{P}\left[\frac{1}{M}\sum_{\ell=0}^{f_i-m}\sum_{k=0}^{M-1} n_{l,k} \leq -\frac{1-6\eta}{2}\right] \\
&\leq e^{-\frac{M(f_i-m)(1-4\eta)^2}{16(f_i-m)^2}} \\
&\leq e^{-\frac{M(1-6\eta)^2}{16 f_i}} \\
&\approx e^{-\frac{N^{\mu-\alpha}(1-6\eta)^2}{16}}.
\end{aligned}$$

□

APPENDIX B
TEST APPENDIX

Lemma 11.

Lemma 12.

REFERENCES

[1] A. Andoni, H. Hassanieh, P. Indyk, and D. Katabi, "Shift finding in sub-linear time," in *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 457–465, Society for Industrial and Applied Mathematics, 2013.

[2] A. Amir, M. Lewenstein, and E. Porat, "Faster algorithms for string matching with k mismatches," *Journal of Algorithms*, vol. 50, no. 2, pp. 257–275, 2004.

[3] R. S. Boyer and J. S. Moore, "A fast string searching algorithm," *Communications of the ACM*, vol. 20, no. 10, pp. 762–772, 1977.

[4] W. I. Chang and T. G. Marr, "Approximate string matching and local similarity," in *Annual Symposium on Combinatorial Pattern Matching*, pp. 259–273, Springer, 1994.

[5] H. Hassanieh, F. Adib, D. Katabi, and P. Indyk, "Faster gps via the sparse fourier transform," in *mobicom*, pp. 353–364, ACM, 2012.

[6] S. Pawar and K. Ramchandran, "A robust r-ffast framework for computing a k-sparse n-length dft in o (k log n) sample complexity using sparse-graph codes," in *Proc. IEEE Int. Symp. Information Theory*, pp. 1852–1856, 2014.