A RECURSIVE ALGORITHM FOR PRUNED BIT-REVERSAL PERMUTATIONS

Mohammad M. Mansour
ECE Department
American University of Beirut
Beirut, Lebanon
Email: mmansour@aub.edu.lb

ABSTRACT
A fast recursive algorithm for pruned bit-reversal permutations is proposed. The algorithm is based on a computationally efficient scheme for evaluating a novel permutation statistic called permutation inliers that counts inlier addresses under pruning. This statistic is computed by evaluating a recursion using integer shift and add operations in logarithmic time complexity. Moreover, a parallel pruned interleaving algorithm based on computing multiple inliers in parallel is proposed. The advantages of the proposed algorithm are reduced latency and reduced memory requirements, which are described in many signal processing and communication applications.

Index Terms—bit-reversal permutations, pruned interleavers.

1. INTRODUCTION
In certain signal processing applications, it is often required to shuffle streaming data [1] into a particular order such as in signal transform (e.g., Cooley-Tukey fast Fourier [2, 3], discrete cosine [4], Hartley transforms [5]), matrix transposition [6, 7], and matrix decomposition algorithms [8]. These shufflings are based on a permutation which is typically data-independent. Examples include bit-reversal, Gray code, linear congruential, and sorting permutations. Such permuters are implemented using double-buffers or in some cases single buffers if the permutation satisfies certain properties, in particular, low permutation order, [1].

However, in many other communications applications, it is sometimes impossible to permute the streaming data before the whole stream is received even if its permutation order is low, due to the fact that the permutation is “address-dependent”. Address generation in this case is the bottleneck. This necessitates double or multiple buffers in order to maintain a desired system processing throughput, which increases the memory requirements. An example of address-dependent permuters are pruned interleavers. Interleavers are used as an adjunct to coding for error correction [9, 10]. They are a subclass of permuters with carefully chosen permutations to break certain patterns in the input sequence, and strategically reposition symbols according to their relevance in protecting the overall sequence against errors. Examples include interleavers in turbo codes [11], channel interleavers in bit-interleaved coded modulation schemes [12], and carrier interleaving for diversity gain in multi-carrier wireless systems with frequency-selective fading and multiple-access interference [13].

A class of computationally efficient interleavers with simple address generation are block interleavers [14] of power-of-2 length $k = 2^n$. They are expressed in closed-form expression by
\[
\rho : Z_k \rightarrow Z_{k_1} \times Z_{k_2}, \rho(j) = k_1 \cdot \pi_1(j \mod k_1) + \pi_2 \left( \frac{j}{k_1} \right),
\]
where $\pi_1 : Z_{k_1} \rightarrow Z_{k_1}$ and $\pi_2 : Z_{k_2} \rightarrow Z_{k_2}$ are basic permutations of lengths $k_1 = 2^{n_1}$ and $k_2 = 2^{n_2}$, respectively, and $k = k_1 k_2$. Here the $k$ symbols are written row-wise into a $k_2 \times k_1$ array and read column-wise after permuting the rows by $\pi_1$ and the columns by $\pi_2$. Example permutations proposed in the literature or adopted in modern communications standards [15, 16, 17] include the bit-reversal permutation (BRP) $\pi(j) = BRP(j \mod k)$ [16] which reverses the order of bits in $j(2)$, and polynomial-based permutations $\pi(j) = f_m(j, k)$ where $f_m(j)$ is a degree-$m$ permutation polynomial [18].

Block interleavers are often required to support several codes with various codeword lengths (not just powers of 2) depending on the input data rate requirements (e.g., recent communication standards [15, 16, 17]). To accommodate for flexible block lengths $\beta$, interleaving is done using a mother interleaver of length $k = 2^n$, where $n$ is the smallest integer such that $\beta \leq k$, such that outlier interleaved addresses greater than $\beta - 1$ are pruned away. However, this pruning operation makes the permutation address-dependent, and creates a serial bottleneck since interleaved addresses are now a function of the permutation as well as the number of pruned addresses. To parallelize this operation, it is essential to characterize the permutation structure with respect to the pruning operation in order to interleave an address without interleaving all its predecessors.

In this paper, we propose a recursive algorithm to speed up pruned interleavers based on bit-reversal permutations. The algorithm is based on an efficient scheme for deriving the so-called “inliers permutation statistic” which counts inlier addresses without traversing all predecessors. This algorithm has logarithmic time-complexity compared to linear complexity for a serially pruned bit-reversal interleaver (PBRI). Moreover, we use this algorithm to parallelize a serial PBRI and reduce latency by a desired parallelism factor. Another important advantage of the proposed algorithm is that it reduces memory buffering requirements and enables on-the-fly interleaving without first storing all the data, then waiting to derive all pruned addresses before shuffling the data. The inliers statistic can be generalized to other permutations, which is the main advantage over our earlier algorithm presented in [19].

2. A BASIC PRUNED PERMUTATION ALGORITHM
Consider the sequence of integers $[k] \triangleq \{0, 1, \ldots, k-1\}$, and let $\pi$ be a permutation on $[k]$. Let $(j_n \cdots j_0)2$ denote the binary representation of an integer $j \in [k]$, let $n = 2^i$, $i$ is the number of bits, and $j_i \in \{0, 1\}$ for $i = 0, \ldots, n-1$. The bit-reversal of $j$ is defined as $\pi_n(j) \triangleq (j_0 j_1 \cdots j_{n-1})2 = \sum_{i=0}^{n-1} j_i 2^{n-1}$.

A bit-reversal interleaver (BRI) maps an $n$-bit number $\alpha$ into another $n$-bit number $y$ such that $y = \pi_n(\alpha)$. The values taken by $\alpha$ and $y$ range from $0$ to $k - 1$, where $k = 2^n$ is the size of
the interleaver. A pruned BRI (PBRI) maps an $n$-bit number $\alpha < \beta \leq k$ into another $n$-bit number $y < \beta$ according to the bit-reversal rule. The size of the pruned interleaver is $\beta$. Pruned interleavers are used when blocks of arbitrary lengths (other than powers-of-2) are needed. To interleave a block of size $\beta$, a mother interleaver whose size is the smallest power-of-2 that is $\geq \beta$ is selected and pruned. Hence, in the following, we assume that $k/2 < \beta < k$.

There are several ways to prune addresses from the mother interleaver. One method is to ignore positions beyond $\beta - 1$ in the permuted sequence, which we consider in this work (see also [20, 21]). Other methods prune addresses beyond $\beta - 1$ in the original sequence, or prune a mixture of addresses from both the original and pruned sequences [21]. Hence any address that maps to an address $\geq \beta$ is dropped and the next consecutive address is tried instead. To determine where an arbitrary address $\alpha$ gets mapped, a serial PBRI (S-PBRI) starts from $w = 0$ and maintains the number of invalid mappings $\delta$ (called the pruning gap) that have been skipped along the way. If $w + \delta$ maps to a valid address (i.e., $\pi\alpha(w + \delta) < \beta$), then $w$ is incremented by 1. If $w + \delta$ maps to an invalid address (i.e., $\pi\alpha(w + \delta) \geq \beta$), $\delta$ is incremented by 1. These steps are repeated until $w$ reaches $\alpha$ and $\pi\alpha(\alpha + \delta)$ is a valid address. Therefore, in a pruned bit-reversal interleaver, $\alpha \rightarrow y = \pi\alpha(\alpha + \delta)$. Algorithm 1 shows the pseudo-code.

**Algorithm 1** Serial PBRI Algorithm: $y = S$-PBRI($k$, $w_1$, $w_2$, $\beta$, $\delta$)

```markdown
\[
\begin{align*}
& w \leftarrow w_1 \\
\text{while } w \leq w_2 \text{ do} \\
& \quad \text{if } \pi\alpha(w + \delta) < \beta \text{ then} \\
& \quad \quad y \leftarrow \pi\alpha(w + \delta) \\
& \quad \quad w \leftarrow w + 1 \\
& \quad \text{else} \\
& \quad \quad \delta \leftarrow \delta + 1 \\
& \text{end if} \\
& \text{end while}
\end{align*}
\]

3. PERMUTATION INLIERS STATISTIC

Permutation statistics have been used to study combinatorial properties of permutations. In [22], a new permutation statistic useful for analyzing pruned interleavers called permutation inliers was introduced. An integer $i \in [k]$ is called an $(\alpha, \beta)$-inlier of $\pi$ if $i < \alpha$ and $\pi(i) < \beta$. We denote by $\text{INL}_{\alpha, \beta}(\pi)$ the set consisting of all $(\alpha, \beta)$-inliers of $\pi$.

$$\text{INL}_{\alpha, \beta}(\pi) = \{ j \in [k] \mid j < \alpha, \pi(j) < \beta \}, \quad 0 < \alpha, \beta \leq k,$$  

and by $\#\text{INL}_{\alpha, \beta}(\pi)$ the number of $(\alpha, \beta)$-inliers of $\pi$. We call determining $\text{INL}_{\alpha, \beta}(\pi)$ the permutation inliers problem. Similarly, an integer $i \in [k]$ is called an $(\alpha, \beta)$-outlier if $i < \alpha$ and $\pi(i) \geq \beta$. OUL$_{\alpha, \beta}(\pi)$ denotes the set of all $(\alpha, \beta)$-outliers, and $\#\text{OUL}_{\alpha, \beta}(\pi)$ their number:

$$\text{OUL}_{\alpha, \beta}(\pi) = [\alpha] - \text{INL}_{\alpha, \beta}(\pi),$$

where ‘$-$’ is the set-difference operator. For example, the (5,7)-inliers of the permutation $\pi = (3 4 2 5 1 6 8)$ are $\text{INL}_{5,7}(\pi) = \{0, 1, 3, 4\}$, while the outliers are $\text{OUL}_{5,7}(\pi) = \{2\}$.

Surprisingly, determining $\text{INL}_{\alpha, \beta}(\pi)$ for arbitrary permutations has largely been unattacked before in the literature. In [23], a solution for linear permutation polynomials based on Dedekind sums [24, 25] was proposed. In [19] a combinatorial solution for bit-reversal permutations based on bit manipulations was presented. Here we present an alternative recursive solution to the problem for bit-reversal permutations based on an efficient evaluation of

$$\#\text{INL}_{\alpha, \beta}(\pi) = \sum_{j=0}^{k-1} \left\lfloor \frac{j - \alpha}{\beta} \right\rfloor \pi(j) - \beta \right\rfloor, \quad (3)$$

which counts the desired inliers. The solution is based on evaluating sums analogous to the well-known Dedekind sums [24]. In [22], it was shown that this solution takes the form

$$\#\text{INL}_{\alpha, \beta} = \frac{\alpha \beta}{k^2} + 1 - \frac{k}{4k}T(k, \alpha, \beta) + K_{\text{INL}}(\alpha, \beta), \quad (4)$$

where $T(k, \alpha, \beta)$ is defined by the following recursion

$$\begin{align*}
T(k, \alpha, \beta) &= \left\lfloor \frac{2T(k/2, \alpha, (\beta - 1)/2) - 4\alpha - K_{\text{INL}}}{2T(k/2, \alpha, \beta/2) + K_{\text{INL}}} \right\rfloor, \\
\text{even},
\end{align*}$$

and 0 if either $\alpha = 0$ or $\beta = 0$. The remaining quantities are given by:

$$K_{\text{INL}} = k \left( \left\lfloor \frac{\beta - \alpha}{k} \right\rfloor - 2 \left\lfloor \frac{\alpha}{k} \right\rfloor - \left\lfloor \frac{\beta - \alpha}{k} \right\rfloor + \delta \left( \frac{\alpha}{k} \right) \right); \quad K_{\text{OUL}} = \left\lfloor \frac{\alpha - \beta}{k} \right\rfloor + \delta \left( \frac{\alpha}{k} \right) + \delta \left( \frac{\beta}{k} \right).$$

Note that since $k$ is a power of 2, only integer shift and add operations are needed to compute (5) and (4), assuming the product of the constants $\alpha \beta$ is computed off-line. Eq. (4) evaluates recursively in at most $\log_2 k - 1$ steps using (5), where the arguments of $T(k, \alpha, \beta)$ are reduced until $T$ reaches 0.

**Example 1** Let $n = 32, k = 2^s = 2^{32}, \alpha = 2^{16} - 1, \beta = 2^{16} + 1$. Then $\alpha \beta/k = (2^{32} - 1)/2^{16}$ and $K_{\text{INL}}$ evaluates to $3/4$ in this case. Using (5), we have $c^* = \pi_{31}(2^{31}) = 2^{31}$ and $T(2^{32} - 1, 2^{16} + 1) = 2T(2^{31}, 2^{16} - 1, 2^{15}) + 2T(2^{30}, 2^{16} - 1, 2^{14})$. These steps are repeated using (5), resulting in $T(2^{32} - 1, 2^{16} + 1) = 4294967300 = 2^{31} + 2^2$. Therefore, using (4) we have $\#\text{INL}_{2^{31} - 1, 2^{32} + 1} = 2$.

4. A RECURSIVE PRUNED PERMUTATION ALGORITHM

The time complexity to determine $\pi$ using the S-PBRI algorithm is $O(k)$. We apply the permutation inliers problem to evaluate the pruning gap $\delta$ more efficiently in order to speed up the pruning process in bit-reversal interleavers. Using the inliers problem formulation, $\delta$ is simply the minimum non-negative integer to be added to $\alpha$ such that $\text{INL}_{\alpha + \delta, \beta}$ has exactly $\alpha$ inliers: $\min \delta \geq 0$ such that $\#\text{INL}_{\alpha + \delta, \beta} = \alpha$.

Out of the first $\alpha$ addresses, there are $\#\text{OUL}_{\alpha, \beta}$ outliers $\geq \beta$. Hence $\delta \geq \#\text{OUL}_{\alpha, \beta}$. Next consider the expanded interval of addresses $\alpha_1 = \alpha + \#\text{OUL}_{\alpha, \beta}$.

**Example 2** Let $n = 32, k = 2^s = 2^{32}, \alpha = 2^{12} + 2^{11}, \beta = 2^{31} + 10$. Applying the MI algorithm, we have $\delta_1 = \#\text{OUL}_{2^{12}, 2^{31} + 10} = 2047$ using (2), (4). Next we expand $\alpha$ to $\alpha + 2047$ and recompute $\delta_2 = \ldots$
Fig. 1. The smallest interval of addresses $\alpha + \delta$ that has exactly $\alpha$ inliers and $\delta$ outliers with respect to $\beta$ when mapped by $\pi_n$.

\[
\#OUL_{2^{12}+2047,2^{31}+10} = 3070. \text{ Similarly at step 3 we have } \delta_3 = \#OUL_{2^{12}+3070,2^{31}+10} = 3582. \text{ The operations are repeated until } t = 12 \text{ with } \delta_{12} = \#OUL_{2^{12}+4093,2^{31}+10} = 4093. 
\]

The gap $\delta$ in Algorithm 2 is initialized to zero for simplicity. There are ways to initialize $\delta$. For example, it can be shown [22] that $\delta$ satisfies the following bound:

\[
\alpha(k/\beta - 1) + W_1 k/\beta \leq \delta \leq \alpha(k/\beta - 1) + W_\alpha k/\beta 
\]

where $W_1$ and $W_\alpha$ are constants. $\delta$ can be initialized with the lower bound, or with the upper bound but the gap in Algorithm 2 must be reduced instead of expanded every iteration.

Algorithm 2 Minimal Inliers (MI) Algorithm: $\delta = MI(k, \alpha, \beta)$

\[
\begin{align*}
& \text{for all } i = 0 \rightarrow p - 1 \\
& \delta_i \leftarrow MI(k, i, \lfloor \beta/p \rfloor, \beta) \\
& y[i, \lfloor \beta/p \rfloor : (i + 1) \lfloor \beta/p \rfloor - 1] \leftarrow S-PBRI(k, i, \lfloor \beta/p \rfloor, (i + 1) \lfloor \beta/p \rfloor - 1, \beta, \delta_i) \\
& \text{end for} \\
& \text{if } \beta \mod p > 0 \text{ then} \\
& \delta_p \leftarrow MI(k, p, \lfloor \beta/p \rfloor, \beta) \\
& y[p, \lfloor \beta/p \rfloor : \beta - 1] \leftarrow S-PBRI(k, p, \lfloor \beta/p \rfloor, \beta - 1, \beta, \delta_{p-1}) \\
& \text{end if}
\end{align*}
\]

The convergence rate of the MI algorithm is $1 - \beta/k$ as Theorem 1 states. The proof is based on the bounds given in (6). The details are omitted due to lack of space.

Theorem 1 (Rate of Convergence) The minimal inliers algorithm converges at a rate $\mu = 1 - \beta/k$.

Using the MI algorithm a parallel PBRI of length $\beta$ with a parallelism factor of $p$ over the S-PBRI can be designed using $p$ (or $p+1$ if $\beta \mod p \neq 0$) S-PBRIs as shown in Algorithm 3. The S-PBRIs are initialized with their respective $\delta$’s using the MI algorithm.

Algorithm 3 Parallel PBRI Algorithm: $y = P-PBRI(k, p, \beta)$

\[
\begin{align*}
& \text{for all } i = 0 \rightarrow p - 1 \\
& \delta_i \leftarrow MI(k, i, \lfloor \beta/p \rfloor, \beta) \\
& y[i, \lfloor \beta/p \rfloor : (i + 1) \lfloor \beta/p \rfloor - 1] \leftarrow S-PBRI(k, i, \lfloor \beta/p \rfloor, (i + 1) \lfloor \beta/p \rfloor - 1, \beta, \delta_i) \\
& \text{end for} \\
& \text{if } \beta \mod p > 0 \text{ then} \\
& \delta_p \leftarrow MI(k, p, \lfloor \beta/p \rfloor, \beta) \\
& y[p, \lfloor \beta/p \rfloor : \beta - 1] \leftarrow S-PBRI(k, p, \lfloor \beta/p \rfloor, \beta - 1, \beta, \delta_{p-1}) \\
& \text{end if}
\end{align*}
\]

5. SIMULATION RESULTS AND CONCLUSIONS

Figure 2 compares the interleaving time of the S-PBRI algorithm and the proposed P-PBRI algorithm as a function of interleaver size, for two values of $p$. As shown from the plots, the time to interleave degrades significantly for the S-PBRI algorithm as $k$ increases. The P-PBRI algorithm attains a speed up improvement of slightly more than $p$ over the S-PBRI algorithm.

Figure 3 illustrates the lower and upper bounds of the pruning gap $\delta$. The plot demonstrates the tightness of the bounds given in (6). Figure 4 shows the convergence rate of the MI algorithm. The asymptotic bounds designate the lower and upper bounds of $\delta$, while the solid line shows the actual values of $\delta$ as the algorithm converges. The rate of convergence depends on the ratio of $\beta/k$, which is the ratio of the pruned interleaver size to the mother interleaver size.

The plots demonstrate the advantages of the proposed MI and P-PBRI algorithms in speeding up the interleaving process when pruning is employed. They eliminate the serial bottleneck of the S-PBRI algorithm. The P-PBRI algorithm can be efficiently utilized to design parallel pruned channel and turbo interleavers employed in modern communications standards such as [15, 16, 17], and hence reduce interleaving latency on the transmitter side and de-interleaving latency on the receiver side.

The proposed scheme to accelerate the interleaving speed of pruned interleavers based on the minimum inliers statistic can be generalized to other permutations structures beyond bit-reversal permutations. An interesting permutation is the one currently employed in LTE [15] which is based on quadratic permutation polynomials (QPP) [18]. The recursive solution in (4) needs to be adapted to QPP which is currently work in progress.

6. REFERENCES


