More on Unscrambling Address Lines

Chang-Chun Lu
Dept of Computer Science and
Information Engineering,
National Cheng Kung University
, No1. TAHSUEH Road,
Tainan 701, Taiwan
E-mail:u6321034@ncnu.edu.tw

Shi-Chun Tsai
*Dept of Computer Science and
Information Engineering,
National Chiao Tung University
, 1001 TAHSUEH Road,
Hsinchu 300, Taiwan
E-mail:sctsai@csie.nctu.edu.tw

Abstract

A writer stores some data in memory accessible via address lines. If an adversary permutes the address lines after the writer leaves the message, then how can a reader find the permutation? This is the so-called *unscrambling address lines problem* [1]. By generalizing the previous approach of Broder et al. [1], we give and analyze a new algorithm, which is parallelizable. We also consider an alternative version of the problem by assuming that the writer have the ability to write at the correct address without the effect of adversary. In this case, we give a very simple algorithm to identify the permutation.

Keyword:permutation, field programmable gate array (FPGA)

1 Introduction

The unscrambling address lines problem [1] arose in the context of FPGA hardware design. An FPGA is a user programmable reconfigurable logic array first introduced in 1986 [2]. The basic logical element of many FPGA is equivalent to a look-up table [3]. There are three parties of the unscrambling address lines problem: a reader, a writer and an adversary. The writer stores logical 0's and 1's in memory with n-bit address lines, which defines 2^n locations for storage. After writing is complete, the adversary permutes the address lines. Therefore, the reader would read the wrong address. Then how can the reader find the permutation? For example, for $n = 4$ there are 16 locations in the memory: if the address lines are set to $x_3x_2x_1x_0 = 1001$, which indicates the 9-th location before the adversary permutes the address lines. If the adversary exchanges the first (x_1) and third (x_3) lines, then $x_3x_2x_1x_0$ becomes 0011– indicating the third location. We consider two possible models for the memory, i.e, write-once and re-writable. In the re-writable model the writer is immune from the effect of adversary and write to the same locations round by round. This version can be stated equivalently: Alice (writer) tries to send some 0-1 signals to Bob (reader) via n channels which the adversary permutes before they communicate. Then how can Alice and Bob design a protocol to uncover the permutation? Broder et al. [1] consider write-once memory model only. Their method has been implemented and used in Compaq Systems Research Center [1]. For each model we give a new efficient and straightforward algorithm with analysis. When the memory is rewritable, it is much simpler to find the permutation and the space can be reduced from $O(n \log n)$ to $O(n)$. The general mechanism of the solution is that: first, we leave some messages at certain addresses in the memory. Then we read the memory at these addresses. According to the output (0 or 1) from the memory, we can divide address lines into two groups. Similarly, we can further divide each group into

*Correspondence may be sent to Prof. Tsai. The work was done while the authors were at National Chi-Nan University and supported in part by the National Science Council of Taiwan under contract NSC 89-2213-E-260-028

two. If the number of address lines is n, after $\log n$ rounds we will divide address lines into n groups and each group contains exactly one line. By collecting the output from the memory in each round, we will know the permutation of each address line. Assume the number of address line is $n = 2^r$. Then the memory locations can be represented with n-dimensional 0-1 vectors. The writer assign 0 or 1 to the locations $x = x_{n-1} \cdots x_1 x_0 \in \{0,1\}^n$. We use π to denote the permutation used by the adversary, where the permutation is on the numbers from 0 to $n-1$. For example, let $n = 4$ (i.e. there are 4 address lines) and let $\pi(0) = 1$,$\pi(1) = 2$,$\pi(2) = 3$,$\pi(3) = 0$. Then $\pi(x_3x_2x_1x_0) = x_2x_1x_0x_3$, which means that when reader tries to read the bit located at $x_3x_2x_1x_0$ it will actually get the bit stored at $x_2x_1x_0x_3$.

We maintain the following invariant: after round k, there are 2^k groups, each group has $n/2^k$ address lines and if line i is in group $(z \bmod 2^k)$, then line i will be in either group $(z \bmod 2^{k+1})$ or group $(z + 2^k \bmod 2^{k+1})$ after the $(k+1)$th round. In each round, groups are independent from each other. Our algorithms make $n \log n$ memory probes to determine the permutation and the addresses used are different from the method by Broder et al [1]. In the write-once model, our advantage over Broder et al. is that we can parallelize our algorithm easily.

2 Preliminary

Let n be the number of address lines. For convenience, let $n = 2^r$. Let π be the permutation that the adversary uses to rearrange the address lines. We try to find the permutation π by probing at certain addresses with specific settings. Let $x = x_{n-1} \cdots x_1 x_0$ be an n-bit address for memory location and $\pi(x) = x_{\pi(n-1)} \cdots x_{\pi(1)} x_{\pi(0)}$. We use the convenient notation δ_R, which is 1 if the relation R is true; 0 otherwise. A key observation is: for any integer j, if $j \bmod 2^{k-1} = z$ then $j \bmod 2^k = z$ or $z + 2^{k-1}$. This observation makes our algorithms more straightforward and is the foundation of Broder's work, but not pointed out in [1].

Let $M(x)$ refer to the value stored at address x. After the writer and adversary, the reader will get the value $M(\pi(x))$ instead of $M(x)$ when probing at x. For $i = 0, \cdots, n-1$, let $e_i = x_{n-1} \cdots x_1 x_0$ denote the address with $x_i = 1$ and $x_j = 0$ for all $j \neq i$. We define $S_w \subseteq \{0, \cdots, n-1\}$, for all 0-1 string w of length at most r, to be the subsets of the labels of address lines. Note that the string w also denotes a binary representation of the set index. Initially, $S_\epsilon = \{0, \cdots, n-1\}$, where ϵ is the empty string. We abuse the notation a little bit by treating all the 0-strings 0^* as zero. Note that ϵ is zero when treated as a number. Let u be a 0-1 string of length $k < r$ and S_u be a subset of the address labels after round k. After round $k+1$, S_u will be evenly split into S_{0u} and S_{1u}. The splitting depends on what we read from the written bits at the specific addresses. Formally, we define S_w's recursively.

Definition2.1 For any positive integer $n = 2^r$, integer $k < r$ and permutation π, define $S_\epsilon = \{0, \cdots, n-1\}$. For any k-bit binary string w, $S_{0w} = \{i | i \in S_w, \pi(i) \bmod 2^{k+1} = w\}$ and $S_{1w} = \{i | i \in S_w, \pi(i) \bmod 2^{k+1} = w + 2^k\}$, where we also treat w as a k-bit binary number.

Lemma2.1 For any $i \in S_w$, we have $\pi(i) \bmod 2^{|w|} = w$ and $|S_w| = n/2^{|w|}$, where $|w|$ is the length or the number of bit of w and let $|\epsilon| = 0$.

Proof: We prove by induction on $|w|$. For $|w| = 0$ (i.e. $w = \epsilon$ and $S_\epsilon = \{0, \cdots, n-1\}$), it is clear that, for any $i \in S_\epsilon$, $\pi(i) \bmod 1 = 0$. Suppose it is true up to $|w| = k$. By the definition of S_{0w} and S_{1w}, it is clear for the case of $|w| + 1$. Similarly, we have $|S_w| = n/2^{|w|}$. ■

Now the problem turns out to be how to find out whether $i \in S_{0w}$ or $i \in S_{1w}$ for each $i \in S_w$ by probing the value at certain memory locations. For the re-writable case, it is rather straightforward. For the write-once case, we need to decide which addresses to set the values. These addresses are independent of the permutation. For reader, the addresses are decided adaptively round by round.

3 Main results

3.1 Re-writable case

First we consider the re-writable case, i.e., the adversary doesn't affect the writer. In this case,

Algorithm 1 (Writer1(k, n))

for $i = 0$ *to* $n-1$ **do** $M(e_i) \leftarrow \delta_{(i \bmod 2^k) \geq 2^{k-1}}$;

Algorithm 2 (Reader1(k, n, z))

for $i = 0$ *to* $n-1$ **do**
  if $(M(e_i) == 1)$ **then** $z_i \leftarrow z_i + 2^{k-1}$;

Figure 1: Writer and reader with re-writable memory model.

the reader and writer only access the addresses e_i's for $i = 0, \cdots, n-1$. In round k ($k = 1, \cdots, r$), the writer sets $M(e_i) = 0$ if $(i \bmod 2^k) < 2^{k-1}$; 1 otherwise. All the other locations won't be used. For $n = 8$, we have the setting as in table 1, where columns 2, 3 and 4 are the values set by the writer in round 1, 2 and 3, respectively. .

Table 1: The values and addresses used in the re-writable case.

address	$M(e_i)$ in round 1	$M(e_i)$ in round 2	$M(e_i)$ in round 3
e_0: 00000001	0	0	0
e_1: 00000010	1	0	0
e_2: 00000100	0	1	0
e_3: 00001000	1	1	0
e_4: 00010000	0	0	1
e_5: 00100000	1	0	1
e_6: 01000000	0	1	1
e_7: 10000000	1	1	1

Lemma3.1 With the above setting, for each address line j, $0 \leq j \leq n-1$, and an arbitrary permutation π we obtain $\pi(j) \bmod 2^k$ after round k.

Proof: We prove by induction on k. Let j indicate any address line. For $k = 1$, we have $M(\pi(e_j)) = M(e_{\pi(j)})$, which is 1 iff $\pi(j) \equiv 1 \pmod 2$. In other words, by probing the value at e_j, indeed $e_{\pi(j)}$, we obtain $\pi(j) \bmod 2^k$. Suppose it is true up to $k-1$, i.e., we know $\pi(j) \bmod 2^{k-1}$ after $k-1$ rounds. Now consider the k-th round. Let $z = \pi(j) \bmod 2^{k-1}$. Then $\pi(j) \bmod 2^k = z$ or $z + 2^{k-1}$. This can be decided by reading $M(\pi(e_j)) = M(e_{\pi(j)})$, which is 0 iff $(\pi(j) \bmod 2^k) < 2^{k-1}$ by the setting for round k. This completes the proof. ■

By the above, after r rounds, we will obtain $\pi(j)$ for each j and recover the permutation π. The algorithms are described in figure 1, where $z = z_{n-1} \cdots z_0$ with $z_i = \pi(i) \bmod 2^{k-1}$ as part of the input. In the first round, all z_i is zero initially. After calling *Reader1*, each z_i is updated to be $\pi(i) \bmod 2^k$.

3.2 Write-once case

In the write-once case, writer can only write to a location once and thus each location cannot be rewritten. We illustrate the idea by the following example in table 2 with $n = 8$ and $\pi = (03526741)$, i.e., $\pi(7) = 0, \pi(6) = 3$, $\pi(5) = 5, \pi(4) = 2$, $\pi(3) = 6, \pi(2) = 7$, $\pi(1) = 4, \pi(0) = 1$.

As we define above $S_\epsilon = \{0, 1, 2, 3, 4, 5, 6, 7\}$. After the first round, we divide S_ϵ into $S_0 = \{7, 4, 3, 1\}$ and $S_1 = \{6, 5, 2, 0\}$. This is done by reading $M(e_i)$, where i is added to S_0 if $M(e_i) = 0$; S_1 otherwise. In other words, address lines indexed by S_0 is permuted to even lines and to odd lines if indexed by S_1. The address lines labeled by S_0 can be permuted to 0 or 2 (mod 4) and lines in S_1 can be permuted to 1 or 3 (mod 4). Thus the further splitting of S_0 and S_1 are independent. To split S_0 we can mask the address lines in S_1 as 1 and for the lines in S_0 we allows only one line with 1. In the second round, writer and reader seemingly use different addresses for writing and reading. But the permutation makes the reader read exactly the locations that have been set values by the writer.

After round 2, we have $S_{00} = \{7, 1\}$ and $S_{10} = \{4, 3\}$ from S_0, and $S_{01} = \{5, 0\}$ and $S_{11} = \{6, 2\}$ from S_1. Similarly, we obtain $S_{000} = \{7\}$, $S_{100} = \{1\}$, $S_{010} = \{4\}$, $S_{110} = \{3\}$, $S_{001} = \{0\}$, $S_{101} = \{5\}$, $S_{011} = \{6\}$, $S_{111} = \{2\}$. From the above singletons, we recover the permutation. Note that each location is written exactly once.

Table 2: The values and addresses used in write-once case.

Write-once Example (n = 8)			$\pi = \binom{76543210}{03526741}$	
Writer address	Value set	Value read	Reader address	Set of address line
				$S_\epsilon = \{0,1,2,3,4,5,6,7\}$
00000001	0	1	00000001	
00000010	1	0	00000010	
00000100	0	1	00000100	
00001000	1	0	00001000	
00010000	0	0	00010000	
00100000	1	1	00100000	
01000000	0	1	01000000	
10000000	1	0	10000000	
				$S_0 = \{1,3,4,7\}$
10101011	0	0	01100111	
10101110	1	1	01101101	
10111010	0	1	01110101	
11101010	1	0	11100101	
				$S_1 = \{0,2,5,6\}$
01010111	0	0	10011011	
01011101	1	1	10011110	
01110101	0	0	10111010	
11010101	1	1	11011010	
				$S_{00} = \{1,7\}$
11101111	0	1	01111111	$S_{000} = \{7\} \rightarrow \pi(7) = 0$
11111110	1	0	11111101	$S_{100} = \{1\} \rightarrow \pi(1) = 4$
				$S_{10} = \{3,4\}$
10111111	0	1	11101111	$S_{010} = \{4\} \rightarrow \pi(4) = 2$
11111011	1	0	11110111	$S_{110} = \{3\} \rightarrow \pi(3) = 6$
				$S_{01} = \{0,5\}$
11011111	0	0	11011111	$S_{001} = \{0\} \rightarrow \pi(0) = 1$
11111101	1	1	11111110	$S_{101} = \{5\} \rightarrow \pi(5) = 5$
				$S_{11} = \{2,6\}$
01111111	0	1	10111111	$S_{011} = \{6\} \rightarrow \pi(6) = 3$
11110111	1	0	11111011	$S_{111} = \{2\} \rightarrow \pi(2) = 7$

More specifically, let S_w be a subset of the address lines. Then by fact 2.1, all $i \in S_w$ has $\pi(i) \bmod 2^{|w|} = w$. Now we need to figure out which addresses to write and to read in order to split S_w into S_{0w} and S_{1w}. Let $u_{n-1} \cdots u_1 u_0$ and $r_{n-1} \cdots r_1 r_0$ indicate the addresses for writer and reader, respectively, where u_i's and r_i's can be 0 or 1. We are interested in the following sets of addresses:

Definition3.1 First define $R_\epsilon = W_\epsilon = \{e_i | i = 0, \cdots, n-1\}$. Given w and S_w, define $R_w = \{r_{n-1} \cdots r_1 r_0 |\ r_j = 1 \text{ for } j \notin S_w; \sum_{j \in S_w} r_j = 1\}$; $W_w = \{u_{n-1} \cdots u_1 u_0 |\ u_j = 1, \text{for } j \bmod 2^{|w|} \neq w \text{ and } \sum_{j \bmod 2^{|w|}=w} u_j = 1\}$.

Both $\sum_{j \in S_w} r_j = 1$ and $\sum_{j \bmod 2^{|w|}=w} u_j = 1$ in the definition make sure that exactly one bit is 1 and the others are 0. Note that W_w has nothing to do with the permutation π. Our writer will set values at the addresses in W_w and reader will probe the addresses in R_w and split S_w into S_{0w} and S_{1w} with the returned values.

Lemma3.2 Given π, w, S_w and n, if $r \in R_w$, then $\pi(r) \in W_w$.

Proof: Let $r = r_{n-1} \cdots r_1 r_0 \in R_w$. Then $\pi(r) = a_{n-1} \cdots a_1 a_0$, where $a_{\pi(i)} = r_i$. With w, we have $j \in S_w$ iff $\pi(j) \bmod 2^{|w|} = w$. So

$$\begin{aligned}
\sum_{j \bmod 2^{|w|}=w} a_j &= \sum_{j \bmod 2^{|w|}=w} r_{\pi^{-1}(j)} \\
&= \sum_{\pi(j') \bmod 2^{|w|}=w} r_{\pi^{-1}(j)}, \\
&\quad \text{where } \pi(j') = j \\
&= \sum_{\pi(j') \bmod 2^{|w|}=w} r_{j'}, \\
&\quad \text{since } j' = \pi^{-1}(j) \\
&= \sum_{j' \in S_w} r_{j'} \\
&= 1
\end{aligned}$$

For $j \notin S_w$, we have $\pi(j) \bmod 2^{|w|} \neq w$ and so $a_{\pi(j)} = 1$, since $r_j = 1$. Thus $\pi(r) \in W_w$. ■

The above lemma is crucial for our approach. Once the addresses are decided, for each $u \in W_w$ the writer sets the corresponding location with 1, if there is a j such that $j \bmod 2^{|w|} = w, u_j = 1$ and $j \bmod 2^{|w|+1} = w + 2^{|w|}$; 0 otherwise. Thus

Algorithm 3 (Writer2(n))

for $i = 0$ *to* $n-1$ **do** $M(e_i) \leftarrow \delta_{i \bmod 2=1}$;
for *all binary string* w *with* $|w| = 1$ *to* $n-1$ **do**
  WriteHelper(w);

Algorithm 4 (WriteHelper(w))

for $i = 0$ *to* $n-1$ **do** $u_i \leftarrow \delta_{i \bmod 2^{|w|} \neq w}$;
/* $u = u_{n-1} \cdots u_0$: *address to be used.*/
$j \leftarrow w$;
for $i = 0$ *to* $\frac{n}{2^{|w|}} - 1$ **do**
  $u_j \leftarrow 1$;
  $M(u) \leftarrow \delta_{i \bmod 2=1}$;
  $u_j \leftarrow 0$;/* *reset the bit for next address* */
  $j \leftarrow j + 2^{|w|}$;

Algorithm 5 (Reader2(w, S_w))

if S_w *has only one element* **then**
  print("$\pi(j) = w$*."); /*Let* j *be the element in* S_w */
else
  for $i = 0$ *to* $n-1$ **do** $r_i \leftarrow \delta_{i \notin S_w}$;
  for *all* $j \in S_w$ **do**
    $r_j \leftarrow 1$;
    if $(M(r) == 1)$ **then** *add* j *to* S_{1w};
    else *add* j *to* S_{0w};
    $r_j \leftarrow 0$; /* *reset* r_j *for next address.* */
  Reader2($0w, S_{0w}$*);*
  Reader2($1w, S_{1w}$*);*

Figure 2: Writer and reader with write-once memory model.

for each $j \in S_w$ the reader accesses the address $r \in R_w$, where $r_i = 0$ for all $i \in (S_w - \{j\})$ and $r_i = 1$ for $i \notin (S_w - \{j\})$. Then it will return the value at $\pi(r) \in W_w$ and j will be put in S_{1w} if the value is 1; otherwise put in S_{0w}. We list the algorithms in figure 2.

It is worthy of mentioning that our method is highly parallel in nature. Once a S_w is available we can further split it into two sets without any information from the other sets. While the method by Broder et al. needs information from another set to split a set. For example, to split a set S_w with their approach, it still needs the input S_{w-1} in order to decide the addresses for reader [1]. Thus, it takes two sets to split a set with their approach.

It is clear that line 2 of *Writer2* dominates the algorithm. Together with *WriteHelper*, the time complexity is $O(\sum_{|w| \leq \log n} n/2^{|w|}) = O(n \log n)$. For *Reader2*, line 4 can be handled in a step with bit manipulation instruction. Hence, the time complexity $T(n)$, starting with S_ϵ can be written with a recurrence relation: $T(n) = 2T(n/2) + O(n)$, which has the solution $T(n) = O(n \log n)$. The correctness of our algorithm can be proved formally by induction. We conclude with the following theorem.

Theorem 1 Writer2 *and* Reader2 *probe* $O(n \log n)$ *locations and correctly return the permutation.*

Based on the independence on splitting the sets S_w's, we can parallelize *Reader2* (i.e., by allowing parallel memory access) and achieve $O(logn)$ time complexity.

4 Conclusion

The original algorithm by Broder et al. [1] is *sequential*. With a closer analysis we improve and obtain a parallelizable algorithm. For write-once memory, the space we used is $O(n \log n)$. For rewritable memory, we reduce the cost of space to $O(n)$ by reusing memory.

References

[1] Andrei Broder, Michael Mitzenmacher, Laurent Mall, *Unscrambling Address Lines*, SODA 1999: 870-871

[2] W. S. Carter & Al. , *A user programmable reconfigurable logic array*, in Proceedings of the IEEE 1986 Custom Integrated Circuits Conference., May 1986, pp. 238-235.

[3] *The programmable logic data book 1998.* Xilinx Inc., San Jose, CA, 1998. Available on line via http://www.xilinx.com/partinfo/databook.htm .