APPENDIX A
PROOF OF THE CORRECTNESS

We now prove Short Code can be recovered from up to two disk failures. Since stripes are independent on each other in terms of redundancy relations and single disk failures can be easily recovered by horizontal parity chains, we only demonstrate how Short Code reconstruct from double disk failures in one stripe.

Without loss of generality, we denote the two failed disks as f_1 and f_2, where $0 \leqslant f_1 < f_2 \leqslant n-1$. There are two kinds of double disk failures depending on whether the last disk fails (i.e., $f_2 = n-1$).

Case I: $f_2 = n-1$.

From the diagonal construction rules, we know that each data element belongs to one and only one diagonal parity chain, while each diagonal parity chain doesn't contain more than one element of each disk. Therefore, for the failed element of f_1, the other elements of each's related diagonal chain are all survived, thus we can reconstruct all the failed elements in f_1. Afterwards, we can reconstruct all the failed element in f_2 by recalculating the parity information based on Equation (1).

Case II: $0 \leqslant f_2 \leqslant n-2$.

According to Lemma 1, two data elements C_{n-2-f_2,f_1} and C_{n-3-f_1,f_2} can be directly recovered by horizontal parity chains, because both of their related horizontal parity chains are only relevant with exact one failed disk. Starting with C_{n-2-f_2,f_1} and C_{n-3-f_1,f_2}, we can reconstruct all failed elements by the following steps.

1) Summary the horizontal relationships among the failed elements.
2) Construct a set $S(n)$ (the number of elements in $S(n)$ needs to be a prime number) and its corresponding cyclic groups $S_m^k(n)$ to help the proof.
3) Prove that starting with C_{n-2-f_2,f_1}, we can recover a part of lost elements in f_2, where the row indexes of these elements equal to the indexes of their related elements in $S_m^k(n)$.
4) Prove that starting with C_{n-3-f_1,f_2}, we can recover another part of lost elements in f_2, where the row indexes of these elements equal to the indexes of the other elements in $S_m^k(n)$.
5) Demonstrate that all the missing elements of f_2 can be recovered in Step (3)(4).

We first give the horizontal relationships between the failed elements (**Step 1**). As shown in Lemma 1, H_i ($0 \leqslant i \leqslant n-2$) is irrelevant with disk $n-2-i$ while the data elements of H_i are the last i elements of row $i-1$ and the first $n-2-i$ elements of row i. Therefore, we can summarize the interacting situations between H_i and disk f_1, f_2 in Table 1.

As shown in Table 1, if $0 \leqslant i < n-2-f_2$ or $n-3-f_1 < i \leqslant n-3$, C_i, f_1 and C_{i,f_2} belong to the same horizontal parity chain (at H_i when $0 \leqslant i < n-2-f_2$, or at H_{i+1} when $n-3-f_1 < i \leqslant n-3$). Otherwise, if $n-2-f_2 < i < n-2-f_1$, C_{i,f_1} and C_{i-1,f_2} belong to the same horizontal parity chain (at H_i). Figure 1 shows the horizontal relationships among the failed elements. In Figure 1, the left column represents f_1, while the right column denotes f_2. We link the failed elements that belong to the same horizontal parity chain.

TABLE 1: The interacting situations between H_i ($0 \leqslant i \leqslant n-2$) and disk f_1, f_2

Range of i	H_i interact f_1 at	H_i interact f_2 at
$[0, n-2-f_2)$	C_{i,f_1}	C_{i,f_2}
$n-2-f_2$	C_{i,f_1}	None
$(n-2-f_2, n-2-f_1)$	C_{i,f_1}	C_{i-1,f_2}
$n-2-f_1$	None	C_{i-1,f_2}
$(n-2-f_1, n-3]$	C_{i-1,f_1}	C_{i-1,f_2}

We then build an auxiliary set $S(n)$ to help our proof (**Step 2**). Firstly, we give some definitions and lemmas about the auxiliary set.

***S*(*n*)**: An auxiliary set with n elements which are labeled as the $0th$ element to $(n-1)th$ element. n needs to be a prime number.

Gap: The cycling distance from one element of $S(n)$ to another one element. In mathematics, the gap from the ath element to the bth element is $< b-a >_n$.

Traverse: starting with a certain element of $S(n)$, e.g., the ath element, "traverse b elements" means to find an element that the gap from the ath element to this element is exact b. Therefore, after traversing we get to the $< a+b >_n th$ element.

Traverse back: Traversing back is the inverse operation of traversing. Starting with the ath element and traversing b elements back, we will reach the $< a-b >_n th$ element.

$S_m^k(n)$: Starting with the kth element ($0 \leqslant k \leqslant n-1$), we cyclically traverse $S(n)$ back with a gap of m ($1 \leqslant m \leqslant n-1$). Each traversing back will reach a certain element, we add this element to a sequence $S_m^k(n)$. After

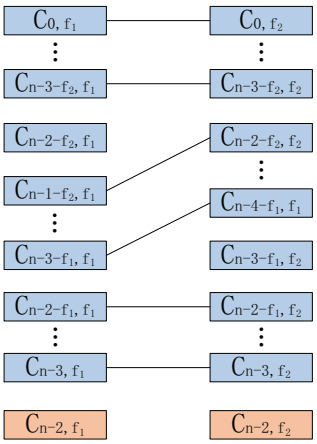

Fig. 1: Horizontal relationships among the failed elements.

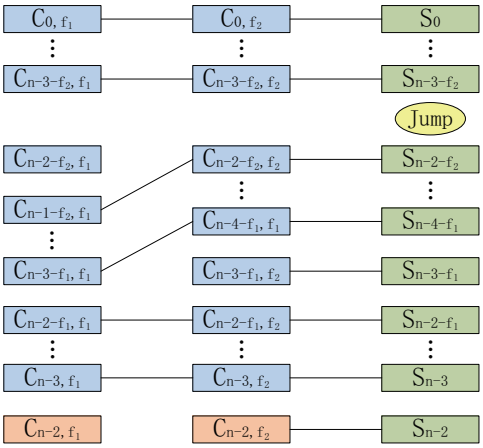

Fig. 2: The mapping relationships among S_i and the failed elements of disk f_2.

n times traversing back operation, $S_m^k(n)$ contains n elements. There is a lemma for $S_m^k(n)$.

Lemma 2: $S_m^k(n)$ contains all the elements of $S(n)$, where the $(n-2)th$ element is the $< k+m >_n th$ element of $S(n)$, and the last ($(n-1)th$) element is the kth element of $S(n)$.

Proof: By assuming that the xth and yth ($0 \leqslant x < y \leqslant n-1$) element of $S_m^k(n)$ are the same element in $S(n)$, we can get a equation:

$$k-(x+1)\cdot m \equiv k-(y+1)\cdot m \pmod{n} \qquad (4)$$

Equation (4) can be simplified as $(y-x)\cdot m \equiv 0 \pmod{n}$. Since n is a prime number and $1 \leqslant m \leqslant n-1$, Equation (4) will never be established when $0 \leqslant x < y \leqslant n-1$. Therefore, $S_m^k(n)$ exactly contains all the elements of $S(n)$.

According to the definition of $S_m^k(n)$, the $(n-2)th$ element of $S_m^k(n)$ is the $(< k-(n-1)\cdot m >_n)th$ element of $S(n)$, which is actual the $< k+m >_n th$ element. Similarly, the $(n-1)th$ element of $S_m^k(n)$ is the $(< k-n\cdot m >_n)th$ element of $S(n)$, which is actual the kth element. □

We construct an auxiliary set $S(n)$ in the right column to help our proof. As shown in Figure 2, $S(n)$ contains $n-1$ node elements (which are labeled as S_i, $0 \leqslant i \leqslant n-2$) and one jump element. Each node element link to an element of f_2, where the row indexes of the linked elements are the same. The jump element locates between S_{n-3-f_2} and S_{n-2-f_2}. We construct $S_{f_2-f_1}^{n-2-f_2}(n)$ as the traversing sequence of $S(n)$ starting by "Jump" (which is the $(n-2-f_2)th$ element of $S(n)$). In addition, we assume S_{n-2} is the $\boldsymbol{xth}$ element of $S_{f_2-f_1}^{n-2-f_2}(n)$.

We then recover the lost elements starting by C_{n-2-f_2,f_1} (**Step 3**). Since C_{n-2-f_2,f_1} and $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_2}$ belong to the same diagonal parity chain while other elements of this parity chain are survived, we can reconstruct $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_2}$. Similarly, we can use $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_2}$ and its related horizontal parity chain to reconstruct an element of f_1, which is $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_1}$ or $C_{<n-2-f_2-(f_2-f_1)+1>_{n-1},f_1}$ (determine by horizontal relationships). Based on this element and its related diagonal parity chain, we can also reconstruct another element of f_2, et al.. We use F to denote the recovery sequence on f_2 starting by C_{n-2-f_2,f_1}. There is a lemma for $S_{f_2-f_1}^{n-2-f_2}(n)$ and F:

Lemma 3: Suppose the ith ($0 \leqslant i \leqslant x$) element of $S_{f_2-f_1}^{n-2-f_2}(n)$ is S_j, then the ith element of F is C_{j,f_2}.

Proof: We use mathematical induction to prove this lemma.

First of all, starting with "Jump" and traversing f_2-f_1 elements back, we get to $S_{<n-2-f_2-(f_2-f_1)>_{n-1}}$, which is the first ($0th$) element of $S_{f_2-f_1}^{n-2-f_2}(n)$.

Since C_{n-2-f_2,f_1} and $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_2}$ belong to the same diagonal parity chain, we can reconstruct $C_{<n-2-f_2-(f_2-f_1)>_{n-1},f_2}$, which is the first ($0th$) element of F. Therefore, the first ($0th$) element of $S(n)$ and F follow Lemma 3.

Based on mathematical induction, we assume that the ith element of $S(n)$ and F follow Lemma 3. Specifically, we assume that the ith ($0 \leqslant i \leqslant x-1$) element of $S_{f_2-f_1}^{n-2-f_2}(n)$ is S_j, and the ith element of F is C_{j,f_2}.

Since S_{n-3-f_1} is the $(n-2)th$ element of $S_{f_2-f_1}^{n-2-f_2}(n)$ (because the gap from "Jump" to S_{n-3-f_1} is f_2-f_1) and S_{n-2} is the xth element of S_{n-3-f_1}, they will certainly not occur when $0 \leqslant i \leqslant x-1$. Therefore, we discuss the different value of j in two cases.

Case 1: $j \in [n-2-f_2, n-3-f_1)$.

In this case, the range of j guarantees that the gap from "Jump" to S_j is no more than f_2-f_1. Based on the definition of $S(n)$, starting with S_j and traversing f_2-f_1 elements back, we reach $S_{<j+1+(f_2-f_1)>_{n-1}}$, which is the $(i+1)th$ element of $S_{f_2-f_1}^{n-2-f_2}(n)$.

We then consider the $(i+1)th$ element of F. As shown in Figure 2, in this case C_{j,f_2} and C_{j+1,f_1} belong to the same horizontal parity chain, thus we can reconstruct C_{j+1,f_1}. Based on C_{j+1,f_1} and its related diagonal parity chain, we can reconstruct $C_{<j+1-(f_2-f_1)>_{n-1},f_2}$, which is the $(i+1)th$ element of F.

Case 2: $j \in [0, n-2-f_2) \cup (n-3-f_1, n-3]$.

Similar as in Case 1, the range of j guarantees that the gap from "Jump" to S_j is no less than f_2-f_1. Therefore, starting with S_j and traversing f_2-f_1 elements back, we get to $S_{<j-(f_2-f_1)>_{n-1}}$, which is the $(i+1)th$ element of $S_{f_2-f_1}^{n-2-f_2}(n)$.

According to the recovery relationships shown in Figure 2, C_{j,f_1} can be reconstructed by C_{j,f_2} and its related horizontal parity chain in this case. Based on C_{j,f_1} and its related diagonal parity chain, we can reconstruct $C_{<j-(f_2-f_1)>_{n-1},f_2}$, which is the $(i+1)th$ element of F.

In summary, when $0 \leqslant i \leqslant x-1$, if the ith element of $S_{f_2-f_1}^{n-2-f_2}(n)$ and F follow Lemma 3, the $(i+1)th$ element

of $S^{n-2-f_2}_{f_2-f_1}(n)$ and F also satisfy this lemma. Therefore, since the first element of $S(n)$ and F follow Lemma 3, from the $0th$ to xth elements of $S(n)$ and F satisfy Lemma 3 as well. □

Another recovery chain starts with C_{n-3-f_1,f_2} (**Step 4**). Since $C_{<n-3-f_1+(f_2-f_1)>_{n-1},f_1}$ can be reconstructed by C_{n-3-f_1,f_2} and its related diagonal parity chain, we can reconstruct an element on disk f_2 by $C_{<n-3-f_1+(f_2-f_1)>_{n-1},f_1}$ and its related horizontal parity chain, which is $C_{<n-3-f_1+(f_2-f_1)>_{n-1},f_2}$ or $C_{<n-3-f_1+(f_2-f_1)-1>_{n-1},f_2}$, and then reconstruct the next element, et al.. We use F' to denote the recovery elements sequence on f_2. By assuming the $\boldsymbol{yth}$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$ is $S_{n-2-(f_2-f_1)}$, there exist two lemmas.

Lemma 4: $y = x + 1$.

Proof: In $S(n)$, since $n-2-(f_2-f_1) \geqslant n-2-f_2$ and the position of $S_{n-2-(f_2-f_1)}$ is below to "Jump", the gap from $S_{n-2-(f_2-f_1)}$ to S_{n-2} is exact $f_2 - f_1$. Therefore, in $S^{n-2-f_2}_{f_2-f_1}(n)$, the next element of S_{n-2} is actual $S_{n-2-(f_2-f_1)}$. Since S_{n-2} is the xth element, $S_{n-2-(f_2-f_1)}$ must be the $(x+1)th$ element, which is the yth element as well. As discussed in Lemma 2, any two elements of $S^{n-2-f_2}_{f_2-f_1}(n)$ are different, thus $y = x + 1$. □

Lemma 5: Suppose the ith ($y \leqslant i \leqslant n-2$) element of $S^{n-2-f_2}_{f_2-f_1}(n)$ is S_j, then the $(n-2-i)th$ element of F' is C_{j,f_2}.

Proof: We use mathematical induction to prove Lemma 5.

First of all, since "Jump" is the $(n-2-f_2)th$ element of $S(n)$, the $(n-2-f_2+(f_2-f_1))th$ element of $S(n)$ is S_{n-3-f_1}, which is the $(n-2)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$ (according to Lemma 2). On the other hand, C_{n-3-f_1,f_2} is the starting element of the recovery chain, which is the first ($0th$) element of F'. Therefore, when $i = n-2$, $S^{n-2-f_2}_{f_2-f_1}(n)$ and F' follow Lemma 5.

Based on mathematical induction, we assume that the ith ($y+1 \leqslant i \leqslant n-2$) element of $S^{n-2-f_2}_{f_2-f_1}(n)$ and the $(n-2-i)th$ element of F' follow Lemma 5. Specifically, we assume that the ith element of $S^{n-2-f_2}_{f_2-f_1}(n)$ is S_j, while the $(n-2-i)th$ element of F' is C_{j,f_2}.

Since $S_{<n-2-f_2-(f_2-f_1)>_{n-1}}$ is the first element of $S^{n-2-f_2}_{f_2-f_1}(n)$ (the gap from $S_{<n-2-f_2-(f_2-f_1)>_{n-1}}$ to "Jump" is exact $f_2 - f_1$) and S_{n-2} is the xth element of S_{n-3-f_1}, they will certainly not occur when $x+1 \leqslant i \leqslant n-2$. Since $y = x+1$, we can discuss the different value of j in two cases.

Case 1: $< j + (f_2 - f_1) >_{n-1} \in (n-2-f_2, n-3-f_1]$.

In this case, the range of j guarantee that the gap from S_j to "Jump" is no more than $f_2 - f_1$. Therefore, starting with S_j and traversing $f_2 - f_1$ elements, we get to $S_{<j-1+(f_2-f_1)>_{n-1}}$, which is the $(i-1)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$.

We then consider the $(n-2-(i-1))th$ element of F'. Since C_{j,f_2} and $C_{<j+(f_2-f_1)>_{n-1},f_1}$ belong to the same diagonal parity chain, we can reconstruct $C_{<j+(f_2-f_1)>_{n-1},f_1}$. According to the recovery relationships shown in Figure 2, the range of j guarantees that $C_{<j+(f_2-f_1)>_{n-1},f_1}$ and $C_{<j-1+(f_2-f_1)>_{n-1},f_2}$ belong to the same horizontal parity chain, thus we can reconstruct $C_{<j-1+(f_2-f_1)>_{n-1},f_2}$, which is the $(n-2-i+1)th$ (i.e., $(n-2-(i-1))th$) element of F'.

Case 2: $< j + (f_2 - f_1) >_{n-1} \in [0, n-2-f_2) \cup (n-3-f_1, n-2)$.

In this case, the range of j guarantee that the gap from S_j to "Jump" is no less than $f_2 - f_1$. Therefore, starting with S_j and traversing $f_2 - f_1$ elements, we get to $S_{<j+(f_2-f_1)>_{n-1}}$, which is the $(i-1)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$.

We then consider the $(n-2-(i-1))th$ element of F'. Since C_{j,f_2} and $C_{j+(f_2-f_1),f_1}$ belong to the same diagonal chain, we can reconstruct $C_{j+(f_2-f_1),f_1}$. Similar as in Case 1, the range of j guarantee that $C_{<j+(f_2-f_1)_{n-1},f_1}$ and $C_{<j+(f_2-f_1)>_{n-1},f_2}$ belong to the same horizontal parity chain, thus we can reconstruct $C_{<j+(f_2-f_1)>_{n-1},f_2}$, which is the $(n-2-(i-1))th$ element of F'.

In summary, when $y+1 \leqslant i \leqslant n-2$, if the ith element of $S^{n-2-f_2}_{f_2-f_1}(n)$ and the $(n-2-i)th$ element of F' follow Lemma 5, the $(i-1)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$ and the $(n-2-(i-1))th$ element of F' also satisfy Lemma 5. Therefore, since the $(n-2)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$ and the $0th$ element of F' satisfy Lemma 5, from yth to $(n-2)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$ and their linked elements of F' satisfy Lemma 5 as well. □

We now demonstrate that all the lost elements of f_2 can be recovered by the recovery chain either in Lemma 3 or in Lemma 5 (**Step 5**). It is easy to see that we can reconstruct $x+1$ different elements of f_2 based on Lemma 3, where the row indexes equal to the indexes of the $0th$ to xth elements of $S^{n-2-f_2}_{f_2-f_1}(n)$. Similarly, we can reconstruct $n-y-1$ (i.e., $n-x-2$) different elements of f_2 based on Lemma 5, where the row indexes equal to the indexes of yth element (i.e., the $(x+1)th$ element) to $(n-2)th$ element of $S^{n-2-f_2}_{f_2-f_1}(n)$. Therefore, we can merge the two recovery sequences (F and F') as one recovery sequence, where the row indexes of the new sequence's elements equal to the indexes of the first $n-1$ elements of $S^{n-2-f_2}_{f_2-f_1}(n)$. As Lemma 2 discussed, any two elements of $S^{n-2-f_2}_{f_2-f_1}(n)$ are different, thus we can reconstruct $n-1$ different elements of f_2. Since f_2 contains exact $n-1$ rows, all failed elements of f_2 are reconstructed. Afterward, we consider the failed elements of f_1. Since all elements of f_2 are recovered, each element of f_1 can be directly reconstructed by its related horizontal parity chain or diagonal parity chain, either. Now, all the failed elements are recovered.

In conclusion, for any case of two disk failures situations, we can reconstruct all the failed elements by the repairing methods discussed in Case I and Case II, which illustrates that Short Code can tolerate any two disk failures.