ELSEVIER

Discrete Applied Mathematics 116 (2002) 231–242

DISCRETE APPLIED MATHEMATICS

Group testing and fault detection for replicated files

F.K. Hwang[a], Wenan Zang[b,*,1]

[a] *Department of Applied Mathematics, Chiao Tung University, Hsinchu 30050, Taiwan, ROC*
[b] *Department of Mathematics, University of Hong Kong, Hong Kong, China*

Received 14 September 1999; revised 26 July 2000; accepted 7 August 2000

Abstract

A file in a distributed database system is replicated on M sites and may contain corrupted pages. The purpose of this paper is to apply a group testing technique to detect corrupted pages in these replicated files. Our detection scheme, based on the structure of the Reed–Solomon code as proposed by Abdel-Ghaffar and El Abbadi, is optimal for $M \geqslant 4$ and has performance guarantee of $\frac{7}{6}$ for $M = 3$.

Keywords: Group testing; Reed–Solomon code; Maximum clique; Depth-first search

1. Introduction

Group testing has a long history, and from the beginning it has been closely tied to large-scale blood testing. Modern applications of group testing are made to many important areas such as experimental designs, coding theory, multiaccess communication, and computational complexity. The interested readers are referred to the book of Du and Hwang [6] for more information about this subject. The present paper is devoted to an application of group testing in distributed database systems, where large files are often replicated and stored at remote sites to permit easy access or to prevent accidental loss of information. Since data in a file can be corrupted due to many reasons, it is desirable to compare the files from time to time to detect faults, group testing techniques are thus employed to meet such needs by various authors. One popular technique, proposed by Metzner and Abidi [11], is the so-called *method of combined signatures*. A file is divided into pages of standard size; a binary parity sequence, called a *signature*, is derived for each page. It is assumed that two copies of a page agree if and only if their signatures agree. A *combined signature* is a weighted sum of a subset of signatures. Group testing is based on combined signatures: all disagreeing

* Corresponding author.
E-mail address: wzang@maths.hku.hk (W. Zang).
[1] Supported in part by CRCG Grant 10202722, RGC Grant 338/024/0009, and RGC Grant 10202890.

0166-218X/02/$ - see front matter
PII: S0166-218X(00)00325-5

pages between two sites can be detected by comparing combined signatures, and the number of combined signatures exchanged is much smaller than the number of pages in a file as shown by Metzner and Abidi [11].

Many schemes have been proposed (cf. [1–4] and [6–11]) for detecting disagreeing pages between two replicated files. Let N denote the number of pages and let f denote the number of disagreeing pages which is assumed to be known. Abdel-Ghaffar and El Abbadi [3], following an idea of Metzner and Kapturowski [12] of using linear block codes, showed that a one-round exchange of $\min\{N, 2f\}$ combined signatures suffice and the bound is best possible. Later Abdel-Ghaffar and El Abbadi [1] proposed a detection scheme for M replicated files, with $M \geqslant 3$.

In the coordinator-based model, one site is designated as the *coordinator*, say site 1, while other sites $2, \ldots, M$, are referred to as the *participants*; the coordinator exchanges messages with the participants to detect all corrupted pages in the replicated file. Communication is between the coordinator and the participants, that is, participants do not exchange any information. Abdel-Ghaffar and El Abbadi [1] gave an optimal detection scheme which transmits at most $(M-2)\min\{N, f\} + \min\{N, 2f\}$ combined signatures to identify f corrupted pages (or faults) under the assumption $M \geqslant 2f + 1$.

In many applications, f is relatively small compared with N, however M can also be a small number. Thus the condition $M \geqslant 2f + 1$ imposes a severe limit on the number of detectable faults. For instance, in case $M = 3$, only one corrupted page is allowed even though the file has thousands of pages. In this paper, we replace the restriction $M \geqslant 2f + 1$ with a much weaker assumption that *for each page the majority of copies are correct*. Let us point out that this assumption is needed for all detection schemes allowing identical errors and not assuming the existence of an incorruptible site, since otherwise we may not be able to distinguish between the correct pages and the corrupted pages and thus detection failure occurs. Under this assumption, we [8] came up with a non-optimal detection scheme for $M \geqslant 4$ that requires the transmission of at most $(M-1)\min\{N, f\} + \min\{1 + \lceil \sqrt{f} \rceil, 1 + \lfloor (M+1)/2 \rfloor\}\min\{N - f, f\}$ signatures.

The purpose of this paper is to present a new two-round scheme for $M \geqslant 3$ for detecting corrupted pages if the majority of correct copies exist for each page and declaring detection failure otherwise. Our scheme is optimal if $M \geqslant 4$ and has performance guarantee of $\frac{7}{6}$ if $M = 3$.

Theorem. *The minimum number of combined signatures that need to be transmitted in order to identify any f corrupted pages in M copies of a file composed of N pages is* $(M-2)\min\{N, f\} + \min\{N, 2f\}$ *if* $M \geqslant 4$ *and at most* $\min\{N, \lceil 3f/2 \rceil\} + \min\{N, 2f\}$ if $M = 3$.

Let us introduce some notions before presenting our scheme. Throughout, we shall let f_m stand for the number of corrupted pages at site m, let $P_{n,m}$, with $1 \leqslant n \leqslant N$ and $1 \leqslant m \leqslant M$, stand for the nth page of the copy residing in site m, and let $p_{n,m}$ stand for the signature of $P_{n,m}$. Each signature is composed of b bits and thus can

be considered as an element in $GF(2^b)$. Since usually b is much larger than $\log_2 N$, we may assume that different pages have distinct signatures. Let α be a primitive element in the finite field $GF(2^b)$. Then α^j, $j = 1,2,\ldots,N$, are pairwise distinct as $b > \log_2 N$. For each site m and each positive integer j, define the combined signature $sig_{j,m} = \sum_{n=1}^{N} p_{n,m}\alpha^{jn}$, which is the syndrome of a Reed–Solomon code corresponding to the vector $(p_{1,m}, p_{2,m}, \ldots, p_{N,m})$ [5]. Finally, for any vector $(e_1, e_2, \ldots, e_N)$, its *weight* is defined to be the number of non-zero entries. Our detection model is based on the following three facts.

Fact 1. *For any given $E_1, E_2, \ldots, E_N \in GF(2^b)$, the system of equations $\sum_{n=1}^{N} e_n\alpha^{jn} = E_j$, where $j = 1,2,\ldots,N$, has a unique solution.*

Fact 2. *If $(e_1, e_2, \ldots, e_N)$ has weight at most f and if $\sum_{n=1}^{N} e_n\alpha^{jn} = 0$, where $j = 1,2,\ldots,f$, then $e_n = 0$ for each $n = 1,2,\ldots,N$.*

Fact 3. *For any given $E_1, E_2, \ldots, E_J \in GF(2^b)$, where $1 \leqslant J \leqslant N$, the system of equations $\sum_{n=1}^{N} e_n\alpha^{jn} = E_j$ for $j = 1,2,\ldots,J$, has at most one solution of $(e_1, e_2, \ldots, e_N)$ with weight less than or equal to $\lfloor J/2 \rfloor$. This solution can be obtained using a Reed–Solomon decoder* [5].

It follows from Fact 3 that if the number of disagreeing pages between a pair of sites i and j is at most $\lfloor f/2 \rfloor$, then $(e_1, e_2, \ldots, e_N) = (p_{1,i} - p_{1,j}, p_{2,i} - p_{2,j}, \ldots, p_{N,i} - p_{N,j})$ is the unique solution with weight at most $\lfloor f/2 \rfloor$ to the system of equations $\sum_{n=1}^{N} e_n\alpha^{qn} = sig_{q,i} - sig_{q,j}$ for $q = 1,2,\ldots,f$ and the set of disagreeing pages between i and j is precisely the set of non-zero entries in $(e_1, e_2, \ldots, e_N)$.

2. An optimal scheme for $M \geqslant 4$

Suppose that faults are randomly distributed in the M replicated files. Then as M grows, the probability that any two replicated files contain more than half of the faults becomes small. Abdel-Ghaffar and El Abbadi [1] took advantage of this observation to reduce the number of combined signatures needed to be transmitted in the first round, with the possibility of transmitting a few more combined signature in the second round in case the small-probability event occurs. We employ the same idea here for $M \geqslant 4$.

In the case $f \geqslant N$, our algorithm goes as follows: each participant m sends all its N pages signatures $p_{1,m}, p_{2,m}, \ldots, p_{N,m}$ to the coordinator. For each page n and each pair of sites i and j, set $e_{n;i,j} = p_{n,i} - p_{n,j}$, where $1 \leqslant n \leqslant N$ and $1 \leqslant i, j \leqslant M$. Let G_n be a graph with vertex-set $\{1,2,\ldots,M\}$ such that $[i,j]$ is an edge in G_n iff $e_{n;i,j} = 0$. Then each connected component of G_n is a clique since for any three sites i, j and k, we have $e_{n;i,k} = 0$ whenever $e_{n;i,j} = 0$ and $e_{n;j,k} = 0$, so the maximum clique problem on G_n can be solved in linear time by the depth-first search [13]. Let C_n be a maximum clique in G_n for $n = 1,2,\ldots,N$. If $|C_n| \geqslant \lceil (M+1)/2 \rceil$ holds for each page n, then the

majority of sites agree on each page, and thus $F_t = \{n : t \notin C_n\}$ is the set of faults at site t for $t = 1, 2, \ldots, M$. Otherwise, $|C_n| < \lceil (M+1)/2 \rceil$ holds for some page n, we declare detection failure. The total number of signatures sent is $(M-1)N$.

Let us now proceed to the case $f < N$. Our algorithm, followed by detailed analysis, is given below.

Algorithm (*Two-Round with* $f < N$)
SEND (REQUEST $sig_{1,m}, \ldots, sig_{f,m}$) to all participants m
RECEIVE ($sig_{1,m}, \ldots, sig_{f,m}$) from all participants m
FOR each pair of sites i and j, where $1 \leqslant i, j \leqslant M$
Try to compute a vector $e_{i,j} = (e_{1;i,j}, \ldots, e_{N;i,j})$ of weight at most $\lfloor f/2 \rfloor$ as a solution of the system of equations
$\sum_{n=1}^{N} e_{n;i,j} \alpha^{qn} = sig_{q,i} - sig_{q,j}$, *where* $q = 1, 2, \ldots, f$ (1)
Let $w_{i,j}$ denote the weight of the vector $(e_{1;i,j}, \ldots, e_{N;i,j})$ if such a solution exists, and let Ω be the set of all pairs $\{i, j\}$ of sites such that *either*
(a) no solution of (1) with weight at most $\lfloor f/2 \rfloor$ exists *or*
(b) there is a solution of (1) with weight $w_{i,j}$ at most $\lfloor f/2 \rfloor$ satisfying $w_{i,j} > w_{s,t}$ for any pair $\{s, t\}$ of sites disjoint from $\{i, j\}$
END(*FOR*)
IF $\Omega = \emptyset$ **THEN**
FOR each page n, where $1 \leqslant n \leqslant N$
CONSTRUCT a graph G_n with vertex-set $\{1, 2, \ldots, M\}$ such that $[s, t]$ is an edge in G_n iff $e_{n;s,t} = 0$
FIND a maximum clique C_n in G_n
END(*FOR*)
ELSE $\Omega \neq \emptyset$
IF $\Omega = \{\{i, j\}, \{j, k\}, \{k, i\}\}$ for some three sites i, j and k **THEN**
Let m be a site outside $\{i, j, k\}$
FOR each page n and each pair $\{s, t\} \in \Omega$
Replace $e_{n;s,t}$ by $e_{n;s,m} - e_{n;t,m}$
END(*FOR*)
FOR each page n, where $1 \leqslant n \leqslant N$
CONSTRUCT a graph G_n with vertex-set $\{1, 2, \ldots, M\}$ such that $[s, t]$ is an edge in G_n iff $e_{n;s,t} = 0$
FIND a maximum clique C_n in G_n
END(*FOR*)
ELSE some site i is contained in each pair in Ω
FOR each page n, where $1 \leqslant n \leqslant N$
CONSTRUCT a graph $G_n - \{i\}$ with vertex-set $\{1, 2, \ldots, M\} - \{i\}$ such that $[s, t]$ is an edge in $G_n - \{i\}$ iff $e_{n;s,t} = 0$
FIND a maximum clique C_n in $G_n - \{i\}$
END(*FOR*)

IF $|C_n| \geqslant (M-1)/2$ holds for each page n **THEN**
  IF $i = 1$ **THEN**
    Let m be an arbitrary site other than 1
    SEND (REQUEST $sig_{f+1,m}, \ldots, sig_{\min\{N,2f\},m}$) to site m
    RECEIVE ($sig_{f+1,m}, \ldots, sig_{\min\{N,2f\},m}$) from site m
    FOR each page n, where $1 \leqslant n \leqslant N$
      Let $f(n)$ be a site in C_n and set $e_{n;m,f(n)} = 0$ if $f(n) = m$
      Replace $e_{n;1,f(n)}$ by the solution with weight at most f of the following system of equations
      $\sum_{n=1}^{N} e_{n;1,f(n)}\alpha^{qn} = sig_{q,1} - sig_{q,m} + \sum_{n=1}^{N} e_{n;m,f(n)}\alpha^{qn}$ (2)
      where $q = 1, 2, \ldots, \min\{N, 2f\}$
    END(*FOR*)
  ELSE $i \neq 1$
    SEND (REQUEST $sig_{f+1,i}, \ldots, sig_{\min\{N,2f\},i}$) to site i
    RECEIVE ($sig_{f+1,i}, \ldots, sig_{\min\{N,2f\},i}$) from site i
    FOR each page n, where $1 \leqslant n \leqslant N$
      Let $f(n)$ be a site in C_n and set $e_{n;1,f(n)} = 0$ if $f(n) = 1$
      Replace $e_{n;i,f(n)}$ by the solution with weight at most f of the following system of equations
      $\sum_{n=1}^{N} e_{n;i,f(n)}\alpha^{qn} = sig_{q,i} - sig_{q,1} + \sum_{n=1}^{N} e_{n;1,f(n)}\alpha^{qn}$ (3)
      where $q = 1, 2, \ldots, \min\{N, 2f\}$
    END(*FOR*)
    FOR each page n with $|C_n| \geqslant (M-1)/2$ and $e_{n;i,f(n)} = 0$
      SET $C_n = C_n \cup \{i\}$
    END(*FOR*)
  END(*IF*)
  FOR each page n with $|C_n| = (M-1)/2$ and $e_{n;i,f(n)} \neq 0$, where $1 \leqslant n \leqslant N$
    IF $C = \{1, 2, \ldots, M\} - (C_n \cup \{i\})$ is a clique in $G_n - \{i\}$ **THEN**
      Let $g(n)$ be a site in C
      SET $C_n = C \cup \{i\}$ if $e_{n;i,f(n)} = e_{n;g(n),f(n)}$
    END(*IF*)
  END(*FOR*)
 END(*IF*)
END(*IF*)
IF $|C_n| \geqslant \lceil (M+1)/2 \rceil$ for each page n **THEN**
  FOR each site t, where $1 \leqslant t \leqslant M$
    RETURN $F_t = \{n: t \notin C_n\}$ (*F_t is the set of corrupted pages at site t*)
  END(*FOR*)
ELSE(* $|C_n| < \lceil (M+1)/2 \rceil$ for some page n*)
  DECLARE detection failure
END(*IF*)

In the present case, f combined signatures $sig_{q,m} = \sum_{n=1}^{N} p_{n,m}\alpha^{qn}$, are transmitted from each participant m to the coordinator, where $1 \leqslant q \leqslant f$. If a pair of sites contains no more than $f/2$ disagreeing pages, then the comparison of f combined signatures between the pair is sufficient to detect all the disagreeing pages. Any pair satisfying this condition is called *normal* and other pairs are called *abnormal*.

For each pair of sites i and j, the coordinator tries to compute a vector $(e_{1;i,j}, \ldots, e_{N;i,j})$ with weight at most $\lfloor f/2 \rfloor$ as a solution of (1). Recall the algorithm, Ω is the set of all pairs $\{i,j\}$ of sites such that *either* (a) no solution of (1) with weight at most $\lfloor f/2 \rfloor$ exists *or* (b) there is a solution of (1) with weight $w_{i,j}$ at most $\lfloor f/2 \rfloor$ satisfying $w_{i,j} > w_{s,t}$ for any pair $\{s,t\}$ of sites disjoint from $\{i,j\}$. In connection with Ω, the following facts were first established in [8]. For completeness, we furnish the proofs here.

Fact 4. *If $\{i,j\}$ is an abnormal pair, then $\{i,j\}$ is in Ω.*

Proof. We aim to prove that either (a) or (b) stated in the algorithm holds for $\{i,j\}$.

Let A denote the non-empty set of all abnormal pairs. Then A cannot contain two disjoint pairs for otherwise the total number of faults would be greater than f. If $\{i,j\}$ is an abnormal pair, then each pair $\{s,t\}$ disjoint from $\{i,j\}$ is normal, and thus there is a solution with weight $w_{s,t}$ at most $\lfloor f/2 \rfloor$ of (2) with $\{s,t\}$ in place of $\{i,j\}$. Assume that $(e_{1;i,j}, \ldots, e_{N;i,j})$ is a solution of (2) with weight no more than $\lfloor f/2 \rfloor$. Since $(p_{1,i} - p_{1,j}, \ldots, p_{N,i} - p_{N,j})$ is a solution of (2) with weight greater than $\lfloor f/2 \rfloor$, these two solutions are different. Note that $\sum_{n=1}^{N} [e_{n;i,j} - (p_{n,i} - p_{n,j})]\alpha^{qn} = 0$, where $q = 1, 2, \ldots, f$. By Fact 2, there are at least $f+1$ values of n for which $e_{n;i,j} \neq p_{n,i} - p_{n,j}$. For each two sites k and l, let $d_{k,l}$ denote the number of disagreeing pages between them. Then $w_{i,j} + d_{i,j} \geqslant f + 1$, whence $w_{i,j} + f_i + f_j \geqslant f + 1$. So for each pair $\{s,t\}$ disjoint from $\{i,j\}$, we have $w_{i,j} \geqslant f - f_i - f_j + 1 > f_s + f_t \geqslant d_{s,t} = w_{s,t}$, the last equality holds for $\{i,j\}$ is an abnormal pair, $f_i + f_j > \lfloor f/2 \rfloor$, implying $d_{s,t} \leqslant f_s + f_t \leqslant \lfloor f/2 \rfloor$. □

Since Ω contains no two disjoint pairs, the following statement holds.

Fact 5. *Let $\{i,j\}$ be an arbitrary pair of sites in Ω. Then one of the following three cases occurs.*

Case 1. *There is a site k outside $\{i,j\}$ such that $\Omega = \{\{i,j\}, \{j,k\}, \{k,i\}\}$.*

Case 2. *Each pair in Ω contains site i.*

Case 3. *Each pair in Ω contains site j.*

Let us consider Case 1. According to Fact 4, any pair of sites outside Ω is normal. So by Fact 3 all the disagreeing pages between the two sites in this pair have already been detected. Let m be a site outside $\{i,j,k\}$, this site is available as $M \geqslant 4$. Now for each page n and for each pair $\{s,t\} \in \Omega$, replace $e_{n;s,t}$ by $e_{n;s,m} - e_{n;t,m}$ (the coordinator has this information). Since both $\{s,m\}$ and $\{t,m\}$ are outside Ω, we have $e_{n;s,m} = p_{n,s} - p_{n,m}$

and $e_{n;t,m} = p_{n,t} - p_{n,m}$. Thus $e_{n;s,t} = p_{n,s} - p_{n,t}$, which is the genuine difference between the signatures of pages $P_{n,s}$ and $P_{n,t}$. Let G_n be the graph constructed in the algorithm and let C_n be the maximum clique of G_n. If $|C_n| \geqslant \lceil (M+1)/2 \rceil$ for each page n, then $F_t = \{n : t \notin C_n\}$ is the set of corrupted pages at site t; otherwise, we declare detection failure.

Let us turn to consider Case 2. (Case 3 is a mirror image of Case 2, which can be handled similarly.) Let $G_n - \{i\}$ be the graph constructed in the algorithm and let C_n be a maximum clique in $G_n - \{i\}$. If $|C_n| < (M-1)/2$ for some n, then fewer than $\lceil (M+1)/2 \rceil$ sites agree on page n, so detection failure occurs. Now we proceed to the case when $|C_n| \geqslant (M-1)/2$ for each page n.

Subcase 2.1. *i is the coordinator*, *namely* $i = 1$. Let m be an arbitrary site different from 1. For each page n, let $f(n)$ be a site in C_n, since $|C_n| \geqslant (M-1)/2$ and $M \geqslant 4$, $f(n)$ is available. If $f(n) = m$ then set $e_{n;m,f(n)} = 0$; if $f(n) \neq m$ then $e_{n;m,f(n)} = p_{n,m} - p_{n,f(n)}$ as $\{m, f(n)\}$ is a pair outside Ω. Now transmit $\min\{N-f, f\}$ additional combined signatures from site m, and replace $e_{n;1,f(n)}$ by the solution with weight at most f of (2). Since the coordinator has already had $e_{n;m,f(n)}$, the right-most term in (2) makes sense.

Fact 6. *$e_{n;1,f(n)} = p_{n,1} - p_{n,f(n)}$, for $n = 1, 2, \ldots, N$, is the unique solution of* (2) *with weight at most f.*

Proof. Since $\{m, f(n)\}$ is a pair outside Ω, we have $e_{n;m,f(n)} = p_{n,m} - p_{n,f(n)}$. Thus

$$\begin{aligned} sig_{q,m} - \sum_{n=1}^{N} e_{n;m,f(n)}\alpha^{qn} &= \sum_{n=1}^{N} p_{n,m}\alpha^{qn} - \sum_{n=1}^{N} e_{n;m,f(n)}\alpha^{qn} \\ &= \sum_{n=1}^{N} (p_{n,m} - e_{n;m,f(n)})\alpha^{qn} \\ &= \sum_{n=1}^{N} p_{n,f(n)}\alpha^{qn}. \end{aligned}$$

Hence (2) is equivalent to

$$\sum_{n=1}^{N} e_{n;1,f(n)}\alpha^{qn} = sig_{q,1} - \sum_{n=1}^{N} p_{n,f(n)}\alpha^{qn}, \quad \text{where } q = 1, 2, \ldots, \min\{N, 2f\}. \tag{4}$$

By Fact 3, $e_{n;1,f(n)} = p_{n,1} - p_{n,f(n)}$, for $n = 1, 2, \ldots, N$, is the unique solution of (4) with weight at most f, so the statement follows. □

Subcase 2.2. *i is not the coordinator*, *namely* $i \neq 1$. For each page n, let $f(n)$ be a site in C_n, since $|C_n| \geqslant (M-1)/2$ and $M \geqslant 4$, $f(n)$ is available. If $f(n) = 1$

then set $e_{n;1,f(n)}=0$; if $f(n)\neq 1$ then $e_{n;1,f(n)}=p_{n,1}-p_{n,f(n)}$ as $\{1,f(n)\}$ is a pair outside Ω. Now transmit $\min\{N-f,f\}$ additional combined signatures from site i, and replace $e_{n;i,f(n)}$ by the solution of (3). Since the coordinator has already had $e_{n;1,f(n)}$, the right-most term in (3) makes sense. Imitating the proof of Fact 6, we see that (3) is equivalent to

$$\sum_{n=1}^{N} e_{n;i,f(n)}\alpha^{qn}=sig_{q,i}-\sum_{n=1}^{N} p_{n,f(n)}\alpha^{qn},\quad \text{where } q=1,2,\ldots,\min\{N,2f\}. \tag{5}$$

From Fact 3 and (5), we conclude the following statement.

Fact 7. *$e_{n;i,f(n)}=p_{n,i}-p_{n,f(n)}$, for $n=1,2,\ldots,N$, is the unique solution of* (3) *with weight at most f.*

It follows from Facts 6 and 7 that for each page n, we have $e_{n;i,f(n)}=p_{n,i}-p_{n,f(n)}$, which is the real difference between the signatures of the pages $P_{n,i}$ and $P_{n,f(n)}$. Now we are ready to output all the corrupted pages.

For each page n, in case $C_n\geqslant(M-1)/2$ and $e_{n;i,f(n)}=0$, set $C_n=C_n\cup\{i\}$; in case $C_n=(M-1)/2$ and $e_{n;i,f(n)}\neq 0$, let us check if $C=\{1,2,\ldots,M\}-(C_n\cup\{i\})$ is a clique in $G_n-\{i\}$. If yes, let $g(n)$ be a site in C and set $C_n=C\cup\{i\}$ if $e_{n;i,f(n)}=e_{n;g(n),f(n)}$. After obtaining C_n for each page n, let us check the size of C_n. If $|C_n|\geqslant\lceil(M+1)/2\rceil$ holds for each page n, then $F_t=\{n:t\notin C_n\}$ is the set of corrupted pages at site t; otherwise we declare detection failure. The total number of combined signatures sent is $(M-1)f+\min\{N-f,f\}$.

Combining the result that holds for $N>f$ with the result obtained in the case $N\leqslant f$ where $(M-1)N$ signatures are transmitted, we see that our algorithm requires the transmission of at most $(M-2)\min\{N,f\}+\min\{N,2f\}$ signatures.

One popular method for file replication is the primary site model, where a designated copy is called the *primary* copy, while the other $(M-1)$ copies are referred to as the *secondary* copies. All up-dates are directed to the primary copy, which is responsible for updating the secondary copies. The goal is to efficiently compare the secondary copies with the primary copy in order to detect any corruptions in the data stored at the secondary sites. It is assumed that the primary site has the correct copy. In spite of this assumption, Abdel-Ghaffar and El Abbadi [2] showed that at least $(M-2)\min\{N,f\}+\min\{N,2f\}$ signatures need to be transmitted in order to identify up to f corrupted pages. This observation as well as its proof [2] will imply the optimality of our scheme.

Proof of the Theorem. From our algorithm, it follows that to identify f corrupted pages, it suffices to transmit $(M-2)\min\{N,f\}+\min\{N,2f\}$ signatures.

To see the optimality of our scheme, let us appeal to the following fact which was proved by Abdel-Ghaffar and El Abbadi [2] for the primary site model: in the case of $f\leqslant N$, even under the assumption that all faults reside in a participant (but not knowing which one), $(M-2)\min\{N,f\}+\min\{N,2f\}$ is still the minimum number

of combined signatures required to be transmitted. Since this assumption is consistent with our assumption that the majority copies of every page are correct, their lower bound remains to be a lower bound of our model.

As our model is based on Facts 1–3, it is easy to see that any scheme for detecting f corrupted pages can be employed to detect f' corrupted pages for any $f' < f$. Since $(M-2)\min\{N, f\} + \min\{N, 2f\}$ is a valid lower bound for the case $f = N$, it remains valid for the case $f > N$. This completes the proof of our theorem for $M \geqslant 4$.

3. A scheme for $M = 3$

Note that under the assumption, we have $N \geqslant f$. Moreover, each page has at least two correct copies. In the case $N < \lceil 3f/2 \rceil$, each participant m sends all its N pages signatures $p_{1,m}, p_{2,m}, \ldots, p_{N,m}$ to the coordinator, and the remainder of the algorithm is precisely the same as the case $f \geqslant N$ for $M \geqslant 4$. The total number of signatures transmitted is $2N$. Let us proceed to the case when $N \geqslant \lceil 3f/2 \rceil$.

Algorithm

SEND (REQUEST $sig_{1,m}, \ldots, sig_{\lceil 3f/2 \rceil, m}$) to participants $m = 2$ and 3
RECEIVE ($sig_{1,m}, \ldots, sig_{\lceil 3f/2 \rceil, m}$) from participants $m = 2$ and 3
FOR each pair of sites i and j, where $1 \leqslant i, j \leqslant 3$
  Try to compute a vector $e_{i,j} = (e_{1;i,j}, \ldots, e_{N;i,j})$ of weight at most $\lceil 3f/2 \rceil / 2$ as a solution of the system of equations
  $\sum_{n=1}^{N} e_{n;i,j} \alpha^{qn} = sig_{q,i} - sig_{q,j}$, where $q = 1, 2, \ldots, \lceil 3f/2 \rceil$ (6)
  Let $w_{i,j}$ denote the weight of the vector $(e_{1;i,j}, \ldots, e_{N;i,j})$ if such a solution exists, and let $\{i, j\}$ be the pair of sites with the smallest $w_{i,j}$
END(*FOR*)
IF $1 \neq i,\ j$ **THEN**
  SEND (REQUEST $sig_{\lceil 3f/2 \rceil + 1, i}, \ldots, sig_{\min\{N, 2f\}, i}$) to participant i
  RECEIVE ($sig_{\lceil 3f/2 \rceil + 1, i}, \ldots, sig_{\min\{N, 2f\}, i}$) from participant i
  Replace $e_{1,i}$ by a solution $(e_{1;1,i}, \ldots, e_{N;1,i})$ of weight at most f to the system $\sum_{n=1}^{N} e_{n;1,i} \alpha^{qn} = sig_{q,1} - sig_{q,i},\ where = 1,\ 2, \ldots,\ \min\{N, 2f\}$
  FOR each page n
    Replace $e_{n;1,j}$ by $e_{n;1,i} + e_{n;i,j}$
  END(*FOR*)
ELSE $i = 1$
  SEND (REQUEST $sig_{\lceil 3f/2 \rceil + 1, k}, \ldots, sig_{\min\{N, 2f\}, k}$) to participant k with $k \neq i, j$
  RECEIVE ($sig_{\lceil 3f/2 \rceil + 1, k}, \ldots, sig_{\min\{N, 2f\}, k}$) from participant k
  Replace $e_{1,k}$ by a solution $(e_{1;1,k}, \ldots, e_{N;1,k})$ of weight at most f to the system $\sum_{n=1}^{N} e_{n;1,k} \alpha^{qn} = sig_{q,1} - sig_{q,k},\ where = 1,\ 2, \ldots,\ \min\{N, 2f\}$
  FOR each page n
    Replace $e_{n;j,k}$ by $e_{n;1,k} - e_{n;1,j}$
  END(*FOR*)

END(*IF*)
FOR each page n, where $1 \leqslant n \leqslant N$
  CONSTRUCT a graph G_n with vertex-set $\{1,2,3\}$ such that
    $[s,t]$ is an edge in G_n iff $e_{n;s,t} = 0$
  FIND a maximum clique C_n in G_n
END(*FOR*)
IF $|C_n| \geqslant 2$ for each page n **THEN**
  FOR each site t, where $1 \leqslant t \leqslant M$
    RETURN $F_t = \{n : t \notin C_n\}$ (*F_t is the set of corrupted pages at site t*)
  END(*FOR*)
ELSE(*$|C_n| < 2$ for some page n*)
  DECLARE detection failure
END(*IF*)

In our algorithm, each participant $m = 2$ and 3 sends $\lceil 3f/2 \rceil$ combined signatures $sig_{q,m} = \sum_{n=1}^{N} p_{n,m}\alpha^{qn}$ to the coordinator, where $1 \leqslant q \leqslant \lceil 3f/2 \rceil$. If a pair of sites contains no more than $\lceil 3f/2 \rceil/2$ disagreeing pages, then the comparison of $\lceil 3f/2 \rceil$ combined signatures between the pair is sufficient to detect all the disagreeing pages. Let us call any pair satisfying this condition *normal* and other pairs *abnormal*. Let f_i stand for the number of corrupted pages at site i for $i = 1$, 2, and 3. Then $f_1 + f_2 + f_3 = f$. So the pair $\{s,t\}$ of sites with minimum $f_s + f_t$ is normal and hence admits a solution with weight at most $\lceil 3f/2 \rceil/2$ to (6).

Fact 8. *Let $\{i,j\}$ be the pair of sites as specified in the algorithm. Then $\{i,j\}$ is normal.*

Proof. Suppose the contrary: $\{i,j\}$ is abnormal. Then $f_i + f_j > 3f/4$. Since $(p_{1,i} - p_{1,j}, \ldots, p_{N,i} - p_{N,j})$ is a solution of (6) with weight $f_i + f_j > 3f/4$, it must be different from $e_{i,j}$. Note that $\sum_{n=1}^{N} [e_{n;i,j} - (p_{n,i} - p_{n,j})]\alpha^{qn} = 0$, where $q = 1, 2, \ldots, \lceil 3f/2 \rceil$. From Fact 2, it follows that at least $\lceil 3f/2 \rceil + 1$ values of n for which $e_{n;i,j} \neq p_{n,i} - p_{n,j}$. So $w_{i,j} \geqslant \lceil 3f/2 \rceil - (f_i + f_j) + 1$. Now let k be the site different from i and j. Then, without loss of generality, we may assume that $\{j,k\}$ is the pair of sites with minimum $f_j + f_k$. Then $\{j,k\}$ is a normal pair and thus $f_j + f_k = w_{j,k}$. By the above inequality, we have $w_{i,j} \geqslant f/2 + f_k + 1 \geqslant \min\{f_i + f_k, f_j + f_k\} + 1 > f_j + f_k = w_{j,k}$, contradicting the selection of $\{i,j\}$. □

It is deduced from the above fact that for pair $\{i,j\}$, $e_{n;i,j}$ represents the real difference between the signatures $p_{n,i}$ and $p_{n,j}$ for each page n. From the above algorithm, it can be seen that the similar statement holds for $e_{n;s,t}$ when we proceed to the construction of G_n. Thus the validity of our algorithm follows. Clearly, the communication complexity of the algorithm is $\min\{N, \lceil 3f/2 \rceil\} + \min\{N, 2f\}$. Once again from the Abdel-Ghaffar–El Abbadi theorem [2], we conclude that $\min\{N, f\} + \min\{N, 2f\}$ is a lower bound on the minimum number of combined signatures required to be

transmitted. Hence our algorithm has performance guarantee of $\frac{7}{6}$, completing the proof of our theorem. □

4. Remarks

A scheme for detecting corrupted pages in replicated files has been given in this paper. From the Abdel-Ghaffar–El Abbadi theorem [2], it can be deduced that our scheme is optimal for $M \geqslant 4$ and has performance guarantee of $\frac{7}{6}$ for $M = 3$. However, the tight lower bound for the latter case remains unknown. One natural approach to reduce the present communication complexity goes as follows. Let f_i, $1 \leqslant i \leqslant 3$, be defined as before. We propose to call a pair $\{i,j\}$ of sites *normal* if $f_i + f_j \leqslant 2f/3$ and *abnormal* otherwise. Since $f_1 + f_2 + f_3 = f$, we have at least one normal pair (clearly $2f/3$ is a natural cut point). At the first round, each participant is required to transmit $\min\{N, \lceil 4f/3 \rceil\}$ combined signatures. Then try to compute a vector $e_{i,j} = (e_{1;i,j}, \ldots, e_{N;i,j})$ of weight at most $\lceil 4f/3 \rceil/2$ as a solution to (6) with $\lceil 4f/3 \rceil$ in place of $\lceil 3f/2 \rceil$ over there; let $w_{i,j}$ denote the weight of the vector $(e_{1;i,j}, \ldots, e_{N;i,j})$ if such a solution exists. If there are two abnormal pairs, then the pair $\{i,j\}$ with smallest $w_{i,j}$ is normal. (To justify it, we may turn to show that the pair with minimum $f_i + f_j$ has the smallest $w_{i,j}$. Suppose $w_{i,k}$ exists for pair $\{i,k\}$. Then $w_{i,k} \geqslant 4f/3 + 1 - (f_i + f_k) \geqslant 4f/3 + 1 - [2f - (f_j + f_k) - (f_i + f_j)] \geqslant [4f/3 + (f_j + f_k) - 2f] + w_{i,j} + 1 \geqslant w_{i,j} + 1$, as desired.) However, when there is only one abnormal pair, it is hard to derive an abnormal or normal pair according to the weights of solutions to (6), and therefore, it is not so easy to improve the current bound to $\min\{N, \lceil 4f/3 \rceil\} + \min\{N, 2f\}$. We close with a natural question: what is the best lower bound for $M = 3$?

References

[1] K.A.S. Abdel-Ghaffar, A. El Abbadi, Efficient detection of corrupted pages in a replicated file, 12th ACM Symposium on Principles on Distributed Computing, 1993, pp. 219–229.
[2] K.A.S. Abdel-Ghaffar, A. El Abbadi, Comparing multiple file copies with a primary copy using minimal communication, Technical Report TRCS 93-8, Dept. Computer Science, UC Santa Barbara, 1993.
[3] K.A.S. Abdel-Ghaffar, A. El Abbadi, An optimal strategy for comparing file copies, IEEE Trans. Parallel and Distributed Systems 5 (1994) 87–93.
[4] D. Barbará, H. Garcia-Molina, B. Feijoo, Exploiting symmetries for low-cost comparison of file copies, Proceedings of 8th International Conference on Distributed Computing Systems, 1988, pp. 471–479.
[5] R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, Reading, MA, 1984.
[6] D.Z. Du, F. Hwang, Combinatorial Group Testing and its Applications, World Scientific Publishing Co. Pvt. Ltd., Singapore, 1993.
[7] W. Fuchs, K.L. Wu, J.A. Abraham, Low-cost comparison and diagnosis of large remotely located files, Proceedings of Symposium on Reliability Distributed Software and Database Systems, Los Angeles, CA, 1986, pp. 67–73.
[8] F.K. Hwang, W. Zang, Detecting corrupted pages in M replicated large files, IEEE Trans. Parallel Distributed Systems 8 (1997) 1241–1245.
[9] J.J. Metzner, A parity structure for large remotely located data files, IEEE Trans. Comput. 32 (1983) 727–730.
[10] J.J. Metzner, Efficient replicated remote file comparison, IEEE Trans. Comput. 40 (1991) 651–660.

[11] J.J. Metzner, M.A. Abidi, Remote comparison and correction of duplicated data files, Proceedings of the National Telecommunications Conference, 1979, pp. 59.4.1–59.4.4.
[12] J.J. Metzner, E.J. Kapturowski, A general decoding technique applicable to replicated file disagreement location and concatenated code decoding, IEEE Trans. Inform. Theory 36 (1990) 911–917.
[13] R.E. Tarjan, Data Structures and Network Algorithms, SIAM, Philadelphia, PA, 1988.