Paper Title*

*Note: Sub-titles are not captured in Xplore and should not be used

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

5th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

6th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

***Abstract*—RAID-6 is an extension of RAID-5 by adding another parity block. It is designed to tolerate any two concurrent disk failure and maintain a relatively high storage efficiency. The mathematics behind RAID-6 is Galois Field (GF) theory and Reed-Solomon codes. In this project, we develop a RAID-6 based distributed storage system and create a finite field operation library under Python 3.7 envrionment. In addition to basic functionalities, we also implement ...**

***Index Terms*—RAID-6, Galois Field, Reed-Solomon codes, Python**

I. Introduction

The concept of RAID (Redundant Array of Independent Disks) was raised in the paper ”A Case for Redundant Arrays of Inexpensive Disks (RAID)” for the demand for rising the reliability, capacity and speed of storage systems. Instead of reading and writing data in one disk drive, RAID achieves larger width of input/output, and hence improves the performance significantly. Many levels of RAID have been raised since 1970s and are widely used in different data protection requirements. Most RAID implement error-detection drives and employ error protection schemes called ”parity” to provide fault tolerance in one or more disks. Most use simple XOR, but RAID-6 uses two separate parities based respectively on addition and multiplication in a Galois Field and Reed-Solomon error detection. This report focused on RAID-6.

Among all levels of RAID, RAID-5 and RAID-10 are most widely used by industry manufacturers. RAID-10 combines RAID-1 and RAID-0 by dividing data into several parts and mirroring each part into pairs. RAID-10 is designed to tolerate multiple disk failure except two corresponding disks in the mirroring pairs. However, the storage efficiency is at only 50%, which is very low. RAID-5 consists of block-level striping with distributed parity, and the parity information is saved among drives. When facing failure, the loss data can be calculated and rebuilt by distributed parity. However, RAID-5 can only tolerate one disk failure. RAID-6 is designed to tolerate any two concurrent disk failure and maintain a relatively high storage efficiency.

RAID-6 is a private raid-level standard proposed concurrently by several large enterprises. This RAID level is developed on the basis of RAID-5, while unlike RAID-5, there is not only a parity area for sibling data on the drive, but also a parity area for each data block. Two independent parity systems use different algorithms and the data is very reliable. Even if two disks fail at the same time, it does not affect the use of the data, which enhances the disk's fault tolerance. With a RAID-6 based distributed storage system, it is possible to mitigate most of the problems associated with RAID-5.

RAID-6 achieves faster reading performance and higher fault tolerance. All these advantages make larger RAID groups more practical, especially for high-availability systems, as larger-capacity drives take longer to restore. The larger the drive capacities and the larger the array size, the more important it becomes to choose RAID-6 instead of RAID-5. However, RAID-6 is not as popular as other levels of RAID for practical application because of its complicated system and expensive RAID controller. For most small businesses which do not require high security level of data preservation, it is better to use RAID-5 economically. While for businesses demand higher security level of data preservation like data center, it is necessary to implement RAID-6.

In this report, we present a reliable distributed storage system based on RAID-6 under Python 3.7 environment. The mathematical operation in Galois Field is well investigated and created as a library to support RAID-6 controller through practical implementation. The RAID-6 based system support several basic functionalities, such as distributed data storage, failure detection and lost redundancy recovery. On top of the minimal implementation, we also investigate ... The rest of the report is organized as follows: ...

Identify applicable funding agency here. If none, delete this.

II. Overview

III. Problem Specification

The RAID-6 theory is based on the Galois Field mathematics and the Reed-Solomon codes. This section will provide relevant definations and principles in the implementation of a RAID-6 distributed storage system. First, let $D_1, D_2, ..., D_n$ denote n *storage disks* and $C_1, C_2, ..., C_m$ denote m *checksum disks*. Each of this disk holds the same storage capacity. The objective is to define the calculation of C_i such that if any m of $D_1, D_2, ..., D_n, C_1, C_2, ..., C_m$ corrupt. The contents of the corrupted devices can be rebuilt from the non-corrupted devices.

A. Arithmetic over Galois Field

Fields with 2^w elements under closed operations like addition and multiplication are called *Galois Fields* (denoted as **GF**(2^w)). The elements are integers from zero to $2^w - 1$. For example, the field **GF(2)** can be represent as the set $0, 1$. A small field would limit the number of disks possible while a large field would require extremely large tables. For RAID-6, we choose the commonly used field of **GF**(2^8), which allows for a maximum of 255 data disks. The operations in this finite field are illustrated as below:

Addition: The addition field operator ($\oplus$) is performed by bitwise XOR.

Subtraction: The addition and subtraction ($\ominus$) are the same operation. For example, $A \oplus B = A \ominus B$

Multiplication: The multiplication ($\otimes$) is performed by bitwise AND, and can be simplified using logarithms table. The details of setting up this table will be presented later.

Division: Division is defined as multiplication with an inverse like $A/B = A \otimes B^{-1}$

Based on the definitions of the foundamental operations, the following basic rules should be obeyed in this field:

- Addition is commutative: $A \oplus B = B \oplus A$
- Addition is associative: $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
- Multiplication is commutative: $A \otimes B = B \otimes A$
- Multiplication is associative: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- Distributive law: $(A \oplus B) \otimes C = A \otimes C \oplus B \otimes C$

Here, we further explain how to perform multiplication and division in **GF**(2^8). The multiplication and division in this field is much more difficult and harder to implement. Multiplying two field elements is to multiply their corresponding polynominals. To simplify this calculation, we use two look up logarithm tables with length of each equals $2^w - 1$. These tables are defined as *gflog* and *gfilog* and can be generated using Algorithm 1.

- *gflog[]*: This table is defined for the indices 1 to 255, which maps the index to its logarithm in the Galois Field.
- *gfilog[]*: This table is defined for the indices 0 to 254, which maps the index to its inverse logarithm in the Galois Field.

Obviously, *gflog[gfilog[i]] = i*, and *gfilog[gflog[i]] =i*. With these two tables, we can easily multiply two non-zero elements of **GF**(2^8) by adding their logs and then taking the inverse log as given by:

$$A \otimes B = gfilog[gflog[A] + gflog[B]] \tag{1}$$

$$A \otimes B^{-1} = gfilog[gflog[A] - gflog[B]] \tag{2}$$

When w is small, these two tables can accelerate multiplication and division in the Galois Field.

Algorithm 1: Setup logarithm tables

```
Input: $w = 8$, $modulus = 0b100011101$
Output: two logarithm tables
max = 1 << 8
$b = 1$
gflog, gfilog = malloc(max)
for $log = 0$ to max do
    gflog[$b$] = $log$
    gfillog[$log$] = $b$
    $b$ = $b$ << 1
    if $b$ & max then
        $b$ = $b$ ^ $modulus$
```

B. Reed-Solomen Coding

By using Reed-Solomen Coding, we could use more parities to back up our data, not just 2. It could be very helpful when one wants to achieve better data security.

1) Calculating Parities: Suppose we have N data disks and M parity disks. To calculate the parity P_i, we define function F_i:

$$P_i = F_i(d_1, d_2, ..., d_n) = \sum_{j=1}^{n} d_j f_{i,j} \tag{3}$$

If we treat data and parity as vectors, where $D = [d_1, d_2, ..., d_i]$ and $P = [p_1, p_2, ..., p_i]$, we could get a simpler equation:

$$P = FD \tag{4}$$

To calculate P, first, we need to generate the $M \times N$ Vandermonde matrix F where $f_{i,j} = j^{i-1}$

$$F = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & N \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{M-1} & \cdots & N^{M-1} \end{bmatrix} \tag{5}$$

In this way, we could easily get our parities P by applying a matrix multiplication on Galois Field.

2) Recovering Data: To recover our data from disk faliure, we need to define matrix $A = \begin{bmatrix} I \\ F \end{bmatrix}$ and $E = \begin{bmatrix} D \\ P \end{bmatrix}$, where I is a $N \times N$ identity matrix and matrix F, D, P are defined before. So we get the equation:

$$AD = E \tag{6}$$

When a disk or disks encount failure, we could delete the corresponding row in A and E. For instance, we have one failed data disk D_i and one failed parity disk P_j, then we need to delete i_{th} row in I and j_{th} row in F to get a new A'. Likewise, we also need to delete i_{th} row in D and j_{th} rwow in P to get a new E'. Then the equation becomes:

$$A'D = E' \tag{7}$$

What we want is actually D, so the problem becomes to solve the following equation:

$$D = A'^{-1}E' \tag{8}$$

The way we use to calculate the inverse matrix A'^{-1} is Gaussian Elimination, the only difference is we do it in Galois Field. Once we calculate our data D, then by using the method mentioned before: $P = FD$, we could update our parity P if it's necessary.

IV. Implementation

A. Maintaining the Integrity of the Specifications

The IEEEtran class file is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

V. Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections V-A–V-E below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not number text heads—LaTeX will do that for you.

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: "Wb/m^2" or "webers per square meter", not "webers/m^2". Spell out units when they appear in text: ". . . a few henries", not ". . . a few H".
- Use a zero before decimal points: "0.25", not ".25". Use "cm^3", not "cc".)

C. Equations

Number equations consecutively. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{9}$$

Be sure that the symbols in your equation have been defined before or immediately following the equation. Use "(9)", not "Eq. (9)" or "equation (9)", except at the beginning of a sentence: "Equation (9) is . . ."

D. LaTeX-Specific Advice

Please use "soft" (e.g., `\eqref{Eq}`) cross references instead of "hard" references (e.g., `(1)`). That will make it possible to combine sections, add equations, or change the order of figures or citations without having to go through the file line by line.

Please don't use the `{eqnarray}` equation environment. Use `{align}` or `{IEEEeqnarray}` instead. The `{eqnarray}` environment leaves unsightly spaces around relation symbols.

Please note that the `{subequations}` environment in LaTeX will increment the main equation counter even when there are no equation numbers displayed. If you forget that, you might write an article in which the equation numbers skip from (17) to (20), causing the copy editors to wonder if you've discovered a new method of counting.

BibTeX does not work by magic. It doesn't get the bibliographic data from thin air but from .bib files. If you use BibTeX to produce a bibliography you must send the .bib files.

LaTeX can't read your mind. If you assign the same label to a subsubsection and a table, you might find that Table I has been cross referenced as Table IV-B3.

LaTeX does not have precognitive abilities. If you put a `\label` command before the command that updates the counter it's supposed to be using, the label will pick up the last counter to be cross referenced instead. In particular, a `\label` command should not go before the caption of a figure or a table.

Do not use `\nonumber` inside the `{array}` environment. It will not stop equation numbers inside `{array}` (there won't be any anyway) and it might stop a wanted equation number in the surrounding equation.

E. Some Common Mistakes

- The word "data" is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o".
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates).
- Do not use the word "essentially" to mean "approximately" or "effectively".
- In your paper title, if the words "that uses" can accurately replace the word "using", capitalize the "u"; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones "affect" and "effect", "complement" and "compliment", "discreet" and "discrete", "principal" and "principle".
- Do not confuse "imply" and "infer".
- The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the "et" in the Latin abbreviation "et al.".
- The abbreviation "i.e." means "that is", and the abbreviation "e.g." means "for example".

An excellent style manual for science writers is [7].

F. Authors and Affiliations

The class file is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

G. Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced.

H. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation , even at the beginning of a sentence.

TABLE I
TABLE TYPE STYLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a] Sample of a Table footnote.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.