*(**Flipping Bits in Memory…. DRAM Disturbance Errors)***
Yoongu Kim

Abstract

- Major Market items targeted: Intel and AMD DRAM system
- Cause of leakage: Repeated Toggling of a DRAM row's wordline that promotes charge leakage from nearby rows
- Test environment for study and research: FPGA Platform
- Current Statistics: Errors occur within 139k access tries and every 1.7k cells within DRAM are susceptible to errors

Introduction

- Words to Define: Exacerbate, Disturbance
    - Exacerbate:
    - Disturbance:
        - AKA Disturbance Errors
    - PARA:
- Modern DRAM configurability has 3 downsides and 2 potential solutions
    - 1. Limited amount of charge hold
        - Data loss more common
    - 2. Coupling electromagnetic effects
    - 3. Process technology leads to inter-cell cross talk
- DRAM Configuration
    - 2-D Cell array (Each row has a ***Wordline)***
    - Voltage applied to row to activate it for data
        - Too many activations toggle the row on and off repeatedly
        - The constant toggling paves way for charge leakage onto adjacent rows
        - Disturbance error occurs if cells don't return to original charge value
- **Solution**: **PARA -> Minimizes disturbance errors by targeting the most "at risk" rows and refreshing them only**

DRAM Background

- Words to define: Row-Buffer, Sense – Amps, Bank, Rank, Memory Controller, etc.
    - Row-Buffer
    - Sense-Amplifications
    - Bank
    - Rank
    - Memory Controller
    - Timing Constraint
    -
- DRAM Cell Configuration: Transistor (MOSFET ??) and capacitor in series configuration
    - Bitline wire connects all cells in columns/ Wordline wire connects cells in rows
    - Wordline wire has voltage applied to turn on transistors and connect capacitors
    - Capacitors are grounded
    -
- Data Retrieval/Release
    - Data (in charge state) within a row is transferred to row-buffer
    - Row Buffer reads and writes charge to and from the cells

        - Note: Data is loss during the read the process
    - Once access process is complete, worldline's voltage levels are dropped

- DRAM Access
    - Three Stage: Opening Row, Accessing Columns, Closing Row
        - Opening:
            - Wordline wire has voltage applied; Bitline is now connected to row
            - Data transferred to bank's row-buffer
        - Accessing Columns:
            - Read and write access is conducted during stage
        - Closing:
            - Wordline wire has voltage cutoff; row-buffered is now cleared
    - C

Disturbance Errors

- Words to Define:
    - Electromagnetic Coupling
    - Bridges
    - eDRAM
    - Elevated Privileges
- Two concepts these errors violate:
    - 1. Read access should NOT modify data
    - 2. Write access should only modify data at the address opened.

Simulation Demonstration

- Initial Configurations:
    - DDR3 Module (2GB)
    - Intel (Sandy Bridge, Ivy Bridge, and Haswell)
    - AMD (Piledriver)
    - Code La Programming Language – Generates read to DRAM on Data access
- Code Variances

Code 1a	**Code 2a**
Move (X) Move (Y) Clflush (X) Clflush (Y) Mfence Jmp code1a	Mov (X) Clflush (X) Mfence Jmp Code1b

Difference:

Simulation Results

- Great variance between manufacturer platform and date
- Hypothesis proven that activating the row various times cause disturbance errors
- The longer the refresh intervals , the more charge leaked to other cells
- After prolonged activation intervals, the error rates decreased (minimized around 250 ns)
- Poor performance of the wordline circuit leads to poor wordline voltage charge and a decreased chance of disturbance effect.
- Threshold refresh rates is in accordance with DDR3 DRAM set standard

- HW Temperature doesn't affect disturbance errors

Aggressor and Victim Cells in Experiment

- Aggressor: Rows that are repeatedly opened often
    - Three reasons why aggressors cause errors in adjacent rows
        - 1. Wordline Voltage Fluctuation
        - 2. Presence of adjacent rows (which would have to entertain modifying the configuration)
        - 3. Logical Adjacency correlate with physical adjacency
- Victim: Cells that are disturbed by the opened rows
    - For ALL three platforms being tested, there are three victim rows per aggressor row
    - Maximum number of cells disturbed for aggressor row: 110
- Protector: Cells within rows that operate to minimize the disturbance error from occurring
- Concatenating: Linking in a chain or series
- Pattern emerged from '1' -> '0' Errors in the DRAM modules
    - 1 -> Charge State | 0 -> Discharged State
    - Victim cells are likely to LOSE charge
        - Victim Cells must be initially charged to have the error occur
- Keep into consideration that ***BOTH*** aggressor and victim rows contain victim cells, aggressor cells, and protector cells

Proposed Solution to Disturbance Errors

- 1. Make better chips
    - Reconfigure Circuit Design
- 2. Correct Error Manually
    - Implement ECC (Error Correcting Code) modules into chips
- 3. Increase refresh rates
    - Keep refresh interval below refresh threshold (64 ns)
- 4. Make manufactured cells obsolete
    - Reroute victim cells to spare cells
- 5. Retire cells (at user end) → Cloud storage
    - Refresh faulty addresses more quickly
- 6. Identify "hot" rows and refresh neighbors
    - Use Moore Counters/Bloom Filters to monitor when to refresh rows
        - Issue: Hash collisions when using hash functions for counters
- Most "usable" solution: **PARA**
    - ***Probabilistic Adjacent Row Activation***
    - Uses probability to determine when to open up an adjacent row to refresh with the hot row

Conclusion

- **Disturbance Errors are an emerging problem likely to affect current and future computing systems**
- Solutions for DRAM memory would occur at the system-level

Article Summary

This article provides a good starting point for researching DRAM memory modules and how to plan methods of attack using the Row Hammer code. The document starts off by explaining how the DRAM is physically configured in cells at the lowest layer and how data is transported throughout the entire module, guided by Assembly code that is used on the connected FPGA. Kim continues the technical document by explaining his live demonstration of running two simulation codes that exemplifies how the disturbance effect would occur in real time and explains why the "effect" violates the purposes behind memory and associated privileges. From that point, the experiment is conducted, data is collected, the results are explained, and multiple solutions are offered to conclude the document.

Key Points from Article

- DRAM cells are configured by an activating transistor, and a grounded capacitor
    - Voltage is applied to wordline, which turns the capacitor on and data from the cell are transported to the bitline
- DDR3 DRAM standard for Refresh Interval is 64 ns
- Longer Access Intervals correlates to higher data retention rates (after 250 ns)
- DRAM Process for obtaining data: Open row, Access, Close Row
- Data gathered from a row and sent to the row buffer is destroyed during the process
- Internal Temperature does not affect the rate of disturbance errors
- The disturbance errors can only be "found" if the row (and cells) was toggled and voltage was applied
- Common Bit Flip error to keep an eye on: '1' -> '0' (Charged to Discharge)
- Victimized cells from leaked voltage (mostly) comes from one aggressor row
- Disturbance Errors violate two principles of memory
    - 1. Write Access should modify data at the targeted address only
    - 2. Read access should not modify data at any address