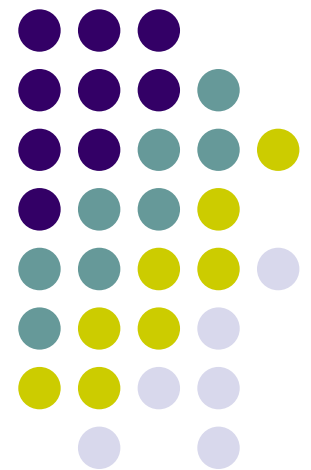


CS257

Introduction to Nanocomputing

Reliable Computation with
Unreliable Elements

John E Savage





Lecture Outline

- The unreliable circuit model
- Reliable gates and redundant circuits
- Control of failure rates
- Redundant circuits of size $O(N \log (N/ \delta))$ simulate circuit of size N achieve error rate δ
- This lecture based Peter Gacs' [notes](#).

The Goal, Problem and Challenge



- **The goal:** To build reliable circuits with unreliable gates.
 - Limit attention to 1-output circuits
- **The problem:** output gates can fail
- **The challenge:** to **avoid the accumulation of errors** at the circuit output.



Goal Restatement

- Prevent circuit failure rate from being more than constant multiple of the gate failure rate.
- If gates fail with probability ε , design circuits so that output failure rate is less than δ , δ close to ε .
 - Such circuits are **(ε, δ) -resilient**.



Circuit Fault Model

- Faults change the value (output) of gates
- V is the set of gates and $Y_v = val_x(v)$ is the (noisy) value at vertex v on input vector \mathbf{x} .
- The values $\{Y_v \mid v \text{ in } V\}$ constitute a random process.
- Let $Z_v = 1$ (0) if gate v does (does not) fail.
(Its output is (is not) different from value computed by the gate on its inputs.)



ϵ -Admissable Configurations

- Let $Z_v = 1$ (0) if gate v in a circuit does (doesn't) fail

Definition for $\epsilon > 0$, configuration $\{Y_v \mid v \text{ in } V\}$ is ϵ -**admissable** if (a) external inputs don't fail and (b) for every set S of non-input nodes,

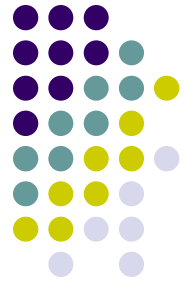
$$P[Z_v = 1 \text{ for all } v \in S] \leq \epsilon^{|S|}$$

- In other words, having faults occur at k different locations is at most ϵ^k . *Gates can't conspire to realize a randomized algorithm!*



Circuit Redundancy

- Given circuit C , the goal is to build a circuit C^* that isn't too much larger than C but is (ε, δ) -resilient when circuit configurations are ε -admissible.
- **New goal:** Find a function $F(N, \delta)$ and $\varepsilon_0 > 0$ such that for $\varepsilon < \varepsilon_0$ and $\delta \geq 2\varepsilon$ for each circuit C of size N there is a circuit C^* that is (ε, δ) -resilient of size at most $F(N, \delta)$. **Redundancy** is $F(N, \delta)/N$.



Building a Reliable Gate

- Make three copies of gate and take majority.
- **Error analysis:** $\varepsilon(\delta)$ = probability of majority (gate copy) failure. New gate fails if majority gate fails (ε) or two or more copies of gate fail ($3\delta^2$). If $\varepsilon + 3\delta^2 \leq \delta$, error rate doesn't increase
- Holds if $\delta \geq 2\varepsilon$ and $\varepsilon < 1/12$.



First (Unrealistic) Approach

Theorem Over complete basis of fan-in 3, every Boolean function of depth t can be realized by an (ϵ, δ) -resilient circuit with $O(3^t)$ gates if $2\epsilon \leq \delta \leq .08$.

Proof *Inductive hypothesis:* given circuit of depth $t \leq T$, can assemble (ϵ, δ) -resilient circuit of depth $2t$. Let output $f = g(f_1(\mathbf{x}), f_2(\mathbf{x}), f_3(\mathbf{x}))$ have depth $T+1$. Build (ϵ, δ) -resilient circuits for each input to g . Take g on their outputs. It's failure rate $\leq 3\delta + \epsilon \leq 4\delta$.

Apply previous slide to 3 copies of these circuits.
Prob. of error $\leq 3(4\delta) + \epsilon \leq \delta$ if $2\epsilon \leq \delta \leq .01$.

Number of gates = $O(3^t)$ for depth t !



A More Realistic Approach

- **Old Goal:** Build a circuit that has the same number of outputs as the unreliable circuit but prevents error accumulation.
- **New Goal: (simple) coded computation**
 - Replicate each output k times.
 - Add circuitry so that with very high probability more than half of the copies of each output produce the correct value.
 - Reliable computation occurs with high probability if there exist reliable k -input majority gates.
 - Reliability increases with k .

Schema for a More Realistic Approach



- For each wire, build **cable** that has k copies of wire.
 - A **wire is tainted** if an error assigned to it.
- For each original gate, create an **executive organ**, that has k copies of the gate.
 - A new **gate is tainted** if it fails or \geq one input is tainted
- For each original gate, create a **restoring organ**.
 - It is designed to decrease the taint of a cable.
 - Built from **compressors**



Tainted Cables

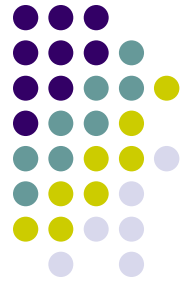
- Cables carry signals from an executive organ
- Inputs to executive organ (EO) are from two cables
- If first (second) cable has e_1 (e_2) errors, output cable can have $e_1 + e_2$ errors.
- Restoring organ reduces number of errors.



Compressors

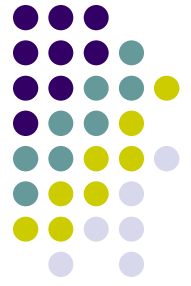
- Compressor must work in noise.
- Build them from bipartite multigraphs
 - Bipartite graphs have two sets of vertices with edges directed from sources to sinks.
 - A multigraph may have multiple edges between pairs of vertices
- Show existence of good compressors using the **probabilistic method**:
 - Construct graphs at random. If probability > 0 of a “good compressor,” then one exists.

Using Compressors as Restoring Organs



- Each output vertex of a compressor computes the majority function on its inputs.

Definition A bipartite multigraph is **d -half-regular** if each output has degree d . Such a graph is a **(d, α, γ, k) -compressor** if for every set E of at most αk inputs, the number of outputs connected to at least $d/2$ inputs of E is at most $\gamma \alpha k$.



Compressors

- View E as errors, $|E| \leq \alpha k$. Majority gates at outputs introduce at most $\gamma \alpha k$ output errors. Thus, the number of errors at output of EO , αk , is reduced to $\gamma \alpha k$, that is by a factor of γ .
- $(5, 0.1, 0.5, k)$ -compressors have output degree 5. Majority operation on outputs decreases 10% input error rate to 5% output error rate.



Existence of Compressors

Theorem For all $\gamma < 1$ and integer d satisfying

$$1 < \gamma (d-1)/2,$$

there is an α such that for all $k > 0$, there exists a (d, α, γ, k) -compressor. (**Note:** Condition fails if $d \leq 3$.)

Proof Consider bipartite graphs with k sources and k sinks. Let $s = \lfloor d/2 \rfloor$. Construct d -half-regular graph: for each output v select d source vertices at random.

Let A , $|A| \leq \alpha k$, be sources. Let E_v be event that output v has $\geq s+1$ edges from A . Let $p = P(E_v)$. Let F_A be event that E_v occurs for $> \gamma \alpha k$ v 's.



Existence of Compressors

Proof (cont.) Let $M = \#$ sets A with $\leq \alpha k$ sources

Let $q = P(\text{no } (d, \alpha, \gamma, k)\text{-compressor exists})$. Then
 $q = P(\exists \geq \text{source set } A, |A| \leq \alpha k, \ni F_A \text{ occurs})$

Clearly, $q \leq MP(F_A)$. If this is ≤ 1 , a (d, α, γ, k) -compressor exists.

Let $\text{bin}(n, p, m) = \sum_{i=m}^n \binom{n}{i} p^i (1-p)^{n-i}$ Then

$p = P(E_v) = \text{bin}(k, \alpha, s+1)$, $P(F_A) = \text{bin}(k, p, \gamma \alpha k)$.

$M = \sum_{i \leq \alpha k} \binom{k}{i} = 2^{-k} \text{bin}(k, .5, (1 - \alpha)k)$



Existence of Compressors

- Compressors exist with following parameters:
 - $\gamma = .4, d = 7, \alpha = 10^{-7}$
 - $\gamma = .4, d = 41, \alpha = .15$

Tainted Outputs at (d, α, γ, k) -Compressor



- Errors at EO output due to tainted inputs.
 - Let $\leq \alpha k$ be number of tainted inputs.
 - Then $\leq \gamma \alpha k$ of majority outputs tainted by tainted inputs.
- If $\leq \rho k$ majority gate errors also occur,
 $\leq (\gamma \alpha + \rho) k$ compressor outputs are tainted
 - $\mu = P(\geq \rho k \text{ maj. gate failures}) = \text{bin}(k, \varepsilon, k\rho)$



Controlling Tainted Outputs

- A k -wire cable is **θk -safe** if $\leq \theta k$ wires are tainted.
- If EO input cables are θk -safe, then $\leq 2\theta k$ EO outputs are tainted by cables. If $\leq \rho\theta k$ of EO gates fail, $\leq (2+\rho)\theta k$ EO outputs tainted.
- Let $\alpha = (2+\rho)\theta$. Then at most $\gamma\alpha k$ of majority gates in (d, α, γ, k) -compressor are tainted by inputs. If $\leq \rho\theta k$ of compressor gates fail, $\leq \gamma(2+\rho)\theta k + \rho\theta k$ outputs are tainted. If $\gamma(2+\rho) + \rho \leq 1$, compressor output cable is also θk -safe.

Probability of Safe Gate Computation

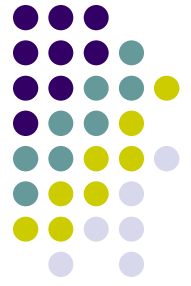


- Let $\alpha = (2+\rho)\theta$ and $\gamma(2+\rho) + \rho \leq 1$.
- If EO input k -wire cables are θk -safe and (d, α, γ, k) -compressor is used, compressor output cable is θk -safe if $\leq \rho\theta k$ compressor gates & $\leq \rho\theta k$ EO gates fail
- Probability that a compressor output cable not θk -safe when all inputs correct $\leq 2\text{bin}(k, \varepsilon, k\rho\theta)$
- Probability that output cable of one or more of the N compute organs is not θk -safe is $\leq 2N \text{bin}(k, \varepsilon, k\rho\theta)$.



Size of Redundant Circuit

- Given a circuit with N gates, a replicated circuit N' can be constructed containing k gate copies (in EOs) plus k majority gates on αk inputs for each gate of N .
- A majority gate is applied to the (each) output cable on k inputs to produce the circuit output(s).
- Majority gates on αk inputs used throughout N' and on its output cable(s) of k inputs.



Size of Redundant Circuit

- Let $c_M(m)$ = number of two-input gates to realize a majority gate on m inputs.
- We construct a *near-majority* gate on 2^p inputs that outputs 1 if $\frac{3}{4}$ of inputs are 1 and 0 otherwise.
 - A majority gate can be constructed by replacing some of the inputs by 0s.

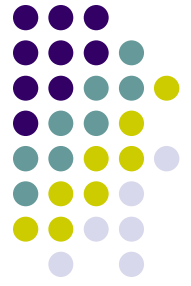


Putting it Altogether

- Inputs are reliable, wires and gates replicated and restored.

Need probability $2N \text{bin}(k, \varepsilon, k\rho\theta)$ that some cable not θk -safe be small.

- Need **output circuit** that produces one output reliably from θk -safe output cable without increasing circuit size or error rate by much.



Output Circuit on 2^k Inputs

- Circuit output has value 1 if $\geq \frac{3}{4}$ of k cable values are 1.
- Realize with circuit of depth $2k$.
- Build fast parallel adder using fan-in 3 gates.

- Let a, b, c, d , and e be binary nos. Form binary numbers d and e so that $d+e = a+b+c$ using two 3-input gates, as follows:

$$d_{i+1} = \lfloor (a_i + b_i + c_i) / 2 \rfloor, e_i = (a_i + b_i + c_i) \bmod 2$$

- d and e need 1 more bit than a, b, c .



Output Circuit

- Start with k 1-bit numbers. Map 3 binary nos. to 2 binary nos.
- Combine with 4th no. to represent sum of 4 inputs by 2 binary numbers.
- Depth 2 circuit reduces # inputs by factor of 2. Length of both results is larger than originals by 1 bit



Output Circuit

- Repeat $k-1$ times to produce 2 output nos. of length $\leq k$ by circuit of depth $2(k-1)$.
- Two most significant bits of 2 outputs decide output value. Increases depth by 2. Depth = $2k$.
- Size of circuit (see Theorem) = $O(3^t) = O(k^7)$ ($t = 4\log_2 k$) which fails with prob. δ if $2\varepsilon \leq \delta \leq .01$



Last Few Pieces

- Circuit with N gates expanded to circuit with $2kN + O(k^7)$ gates. Output circuit fails with probability $\leq \delta$ if $2\varepsilon \leq \delta \leq .01$.
- Make k large so that $2N\text{bin}(k, \varepsilon, k\rho\theta) \leq \delta/3$.
(Holds for $k = O(\log 6N/\delta)/(\rho\theta \log(\rho\theta/\rho\varepsilon_0))$.)
- Set output counting circuit failure rate to 2ε . Thus, failure of output cable or counting circuit is $\delta/3 + 2\varepsilon \leq \delta$ if $\delta \geq 3\varepsilon$.



Summary

- Given unreliable but ε -admissible circuits, there exist an ε_0 such that if $\varepsilon \leq \varepsilon_0$ every failure-free circuit containing N gates can be implemented by (ε, δ) -resilient circuit containing $O(N \log N/\delta)$ gates.
- Unfortunately, the constants in this result are absolutely enormous.
- Although the principle is established, the practice is not.