Stabilizing *D* Flip-flops with Self-Modifiable Differential Equations

Michael Stephen Fiske
HICSS-57

Aemea Institute

January 5, 2024.

"The Purpose of Computing is Insight, not Numbers." [1]

Another Purpose of Computing is to Robustly Perform Tasks.

[1] Richard Hamming. Numerical Methods for Scientists and Engineers. 1962.

Origin of this Paper: HICSS-56

- HICSS-56 paper *"Dynamical Systems that Heal"* asked: How can self-repair be designed to adequately function while actively being attacked by a sentient adversary?
- HICSS-56 peer reviewer 2 stated: *The paper does not seem to cover the case of malicious modification to the ability of an algorithm to detect changes to the code in the first place.*
- HICSS-56 peer reviewer 3 stated: *The novel aspects of the article are focused on self-modifiability for a system of differential equations where the 'damage' done to the system may be the results of other action like white noise where systems are perturbed slightly.*
- Stumbled on "Flip-Flop Gate Model for EEMI Injection."[2]

[2] Valbuena, L., et al. (2019) "Simplified Flip-Flip Gate Model for EEMI Injection." *Intl. Conf. Electromagnetics in Adv. Appl.* 845–850.

Some Electronic Attacks

- Attack on insulin injector sabotages flow of insulin.[3]
- Pacemaker attacks produce dangerous shock commands.[4]
- Injecting clock glitches skips cryptographic instructions.[5]
- Out-of-band signal attacks alter sensor measurements.[6]

[3] Li C., et. al. (2011) "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system." *IEEE Intl. Conf. on e-Health.*

[4] Halperin D., et. al. (2008) "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." *IEEE Symposium on Security and Privacy* .

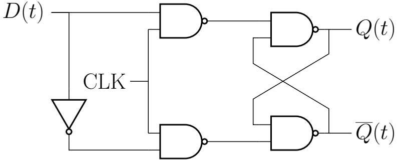
[5] Korak T., Hoefler M. (2014) "On the effects of clock and power supply tampering on two microcontroller platforms." FDTC. 8–17, Sept. 2014.

[6] Giechaskiel I., et. al. (2019) "Taxonomy and challenges of out-of band signal injection attacks and defenses." https://arxiv.org/pdf/1901.06935.pdf.

D Flip-flop

D flip-flops are commonly used in digital electronics.

Flip-flop circuits have two stable physical states.



CLK is clock input. $D(t)$ is data input. $Q(t)$ is output (0 or 1).

Time	CLK	$D(t)$	$Q(t+1)$	$\overline{Q}(t+1)$
t	Rising Edge	0	0	1
t	Rising Edge	1	1	0
t	Non-Rising	$\{0,1\}$	$Q(t)$	$1-Q(t)$

Research Overview

- Start with a differential equations model of a D flip-flop.[7]
- Self-modifiable differential equations help stabilize a D flip-flop during a noise attack.
- A software simulation is provided. No hardware design yet.
- Meta variables can help detect a manipulated flip-flop orbit.
- Meta variables and operators can heal a flip-flop orbit disrupted by noise.

[7] Valbuena L., et al. (2019) "Simplified Flip-Flop Gate Model for EEMI Injection." *Intl. Conf. on Electromagnetics in Adv. Appl.*. 845–850.

Related Work

- LSI Logic scientists created a flip-flop model based on CMOS ASIC technology, using an experimental test circuit.[8]
- Valbuena's flip-flop differential equations model is derived from [8].
- Soft error code correction[9] in flip-flops addresses errors due to radiation from cosmic rays and packaging material. Active electromagnetic attacks by Mallory are not addressed.
- In 2023, introduced self-modifiable differential equations.[10]

[8] Horstmann J.U., et al. (1989) "Metastability behavior of cmos asic flip-flops in theory and test". *IEEE J. Solid Circuits*. 24(1) 146–157.

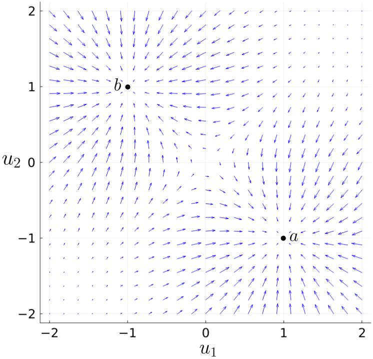
[9] Mitra S., et al. (2007) "Soft Error Resilient System Design through Error Correction." *Intl. Federation for Info. Processing*. 249, 143–156.

[10] Fiske M.S. (2023) "Dynamical Systems that Heal". *HICSS-56*, 6685–6694.

D Flip-flop Differential Equations Model

D flip-flop orbit $u(t) = (u_1(t), u_2(t))$. $\frac{du}{dt} = \left(\frac{du_1}{dt}, \frac{du_2}{dt}\right) =$

$$L_a(u) \begin{pmatrix} \cos\alpha(u) & -\sin\alpha(u) \\ \sin\alpha(u) & \cos\alpha(u) \end{pmatrix} (a - u) + L_b(u) \begin{pmatrix} \cos\beta(u) & -\sin\beta(u) \\ \sin\beta(u) & \cos\beta(u) \end{pmatrix} (b - u).$$



Vector Field $\frac{du}{dt}$

D Flip-flop Differential Equations: $L_p(u)$. $\alpha(u)$, $\beta(u)$

$p = (p_1, p_2)$, $u = (u_1, u_2)$. $||p - u||^2 = (p_1 - u_1)^2 + (p_2 - u_2)^2$.

Symmetric function $L_p(u) = \frac{L_0}{1+e^{c||p-u||^2-d}}$. $c = 0.8$, $d = 1$, $L_0 = 2$.

Build $\alpha(u)$ and $\beta(u)$: $\angle(p, u) = \text{atan2}(p_2 - u_2,\ p_1 - u_1)$.

Fixed points $A = (a_1, a_2)$ and $B = (b_1, b_2)$.

$\phi_B(u) = -\frac{\pi}{2}\tanh(u_2)$.

$\phi_A(u) = \text{atan2}\left(\sin\gamma(u), \cos\gamma(u)\right)$, where $\gamma(u) = \pi - \phi_B(u)$.

Define $g_A(u) = \frac{1}{2} + \frac{1}{2}\tanh(u_1 - \kappa a_1)$, where $\kappa = 1$.

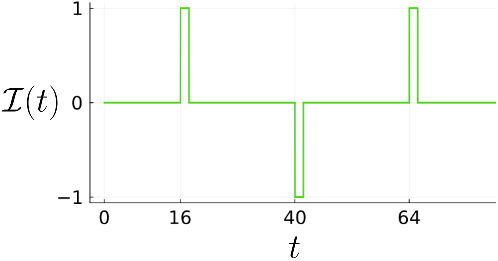
Define $g_B(u) = \frac{1}{2} - \frac{1}{2}\tanh(u_1 - \kappa b_1)$.

Define $\alpha(u) = \frac{1}{2}\ g_A(u)\ (\phi_A(u) - \angle(A, u))$.

Define $\beta(u) = \frac{1}{2}\ g_B(u)\ \left(\phi_B(u) - \angle(B, u)\right)$.

Adding Input

Input pulses store (toggle) the data input in the D flip-flop.

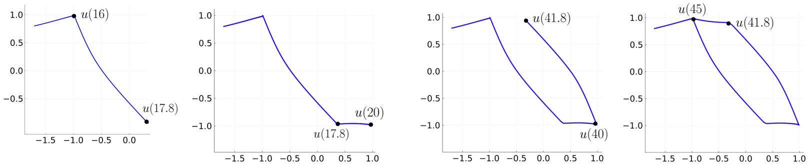


$$\frac{du}{dt} = L_a(u)\begin{pmatrix}\cos\alpha(u) & -\sin\alpha(u)\\ \sin\alpha(u) & \cos\alpha(u)\end{pmatrix}(a-u) + L_b(u)\begin{pmatrix}\cos\beta(u) & -\sin\beta(u)\\ \sin\beta(u) & \cos\beta(u)\end{pmatrix}(b-u) + \begin{pmatrix}K_1\\ K_2\end{pmatrix}\mathcal{I}(t)$$

$c = 0.8,\ d = 1,\ L_0 = 2,\ \kappa = 3.$ Fixed points $a = (1, -1), \quad b = (-1, 1).$

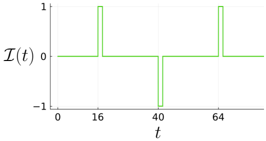
$K_1 = 0.6,\ K_2 = -1.5.$

Toggling the Flip-Flop State



$\begin{pmatrix} K_1 \\ K_2 \end{pmatrix} \mathcal{I}(t)$ models data input $D(t)$ and clock input CLK.

$Q(t) = 0.\quad \overline{Q}(t) = 1. \leftrightarrow\ b = (-1, 1).\quad \mathcal{I}(t) = 0 \leftrightarrow$ row 3 of Table 1.

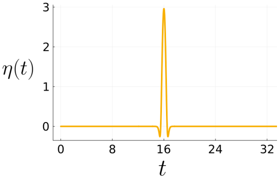


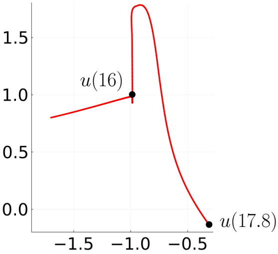
$\mathcal{I}(16) = 1 \leftrightarrow$ row 2. $\quad Q(t+1) := 1$

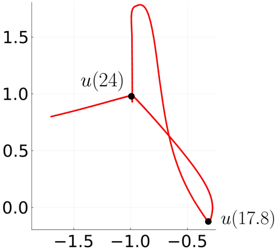
$Q(t+1) = 1.\quad \overline{Q}(t+1) = 0. \leftrightarrow\ a = (1, -1).$

Noise Disrupts Flip-Flop Toggling

Add noise term $+\begin{pmatrix} K_3 \\ K_4 \end{pmatrix}\eta(t)$ to the model. $K_3 = 0$. $K_4 = 1$.







Alice's Goal & Our Approach

Alice's goal: Hinder Mallory from sabotaging her flip-flop.

Our approach is partially motivated by information theory.

Analogous to error-correction bits[11] **add new variables**.

Only mathematical / software methods are explored.
Hardware implementations are not described.

Use self-modifiable differential equations to ameliorate noise.

[11] Hamming R.W. (1950) "Error Detecting and Error Correcting Codes." Bell Technical J. 29(2), 147–160.

Principle of Self-Modifiability in Dynamical Systems

Differential equations are a dynamical system on a manifold.[12]

A set of rules governs a dynamical system:

In a computer program, **each instruction is a rule**.

In a system of differential equations, **each equation is a rule**.

A **self-modifiable dynamical system changes its own rules**:

add new rules to itself; replace rules with new rules; or delete rules.

[12] $\mathbb{C}$ is a 2-D manifold. The unit circle S^1 is a 1-D manifold. Both the torus $S^1 \times S^1$ and sphere S^2 are 2-D manifolds.

Meta Variables & Meta Operators

A *meta operator* specifies how to self-modify an equation.

A meta operator requires a specific time to execute.

A *meta variable* ω helps detect an event.

A function $f(t, \omega, \frac{d\omega}{dt})$ is integrated with respect to time.

$$\frac{d\omega}{dt} = \frac{du_4}{dt} - \frac{du_2}{dt}. \quad \text{Time } s_2 = \inf \{\tau \geq 0 : | \int_0^{\tau} \frac{d\omega}{dt}\, dt| \geq \theta_2\}.$$

A *detectable event*: integral first goes beyond threshold θ_2.

A meta operator corresponding to ω executes at time s_2.

Alice Adds Healing Variables

Alice adds healing variables u_3, u_4. u_1, u_2 are signal variables.

Set $\nu_1(t) = (u_1(t), u_2(t))$ and $\nu_2(t) = (u_3(t), u_4(t))$. For $i = 1, 2$:

$$\frac{d\nu_i}{dt} = L_a(\nu_i) \begin{pmatrix} \cos\alpha_i(\nu_i) & -\sin\alpha_i(\nu_i) \\ \sin\alpha_i(\nu_i) & \cos\alpha_i(\nu_i) \end{pmatrix} (a - \nu_i) \;+\; \begin{pmatrix} K_{i,1} \\ K_{i,2} \end{pmatrix} \mathcal{I}(t)$$
$$L_b(\nu_i) \begin{pmatrix} \cos\beta_i(\nu_i) & -\sin\beta_i(\nu_i) \\ \sin\beta_i(\nu_i) & \cos\beta_i(\nu_i) \end{pmatrix} (b - \nu_i) \;+\; \begin{pmatrix} K_{i,3} \\ K_{i,4} \end{pmatrix} \eta_i(t)$$

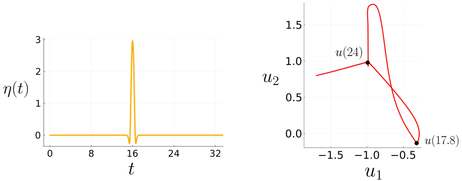
Boundary conditions $u_1(0) = u_3(0)$ and $u_2(0) = u_4(0)$.

Input constants $K_{1,1} = K_{2,1} = 0.6$, and $K_{1,2} = K_{2,2} = -1.5$.

Noise constants $K_{1,3} = 0$, and $K_{1,4} = 1$: noise only disrupts signal variable u_2. Meta operator 2 assumes there is no noise injection on variables u_3, and u_4, so $K_{2,3} = K_{2,4} = 0$.

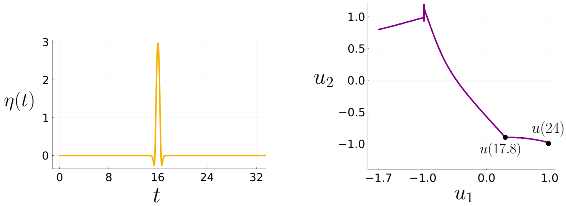
Meta Operator 2 Heals Noise Attack

No Healing. Toggle Fails.



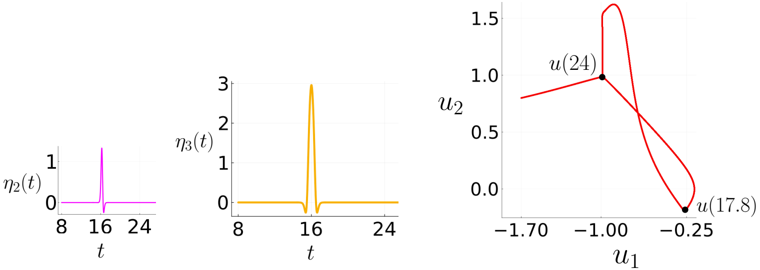
Meta Operator 2. $\frac{d\omega_2}{dt} = \frac{du_4}{dt} - \frac{du_2}{dt}$. $\omega_2(0) = 0$. $\theta_2 = 0.2$.

If $|\omega_2(t)| \geq \theta_2$, set $\frac{du_2}{dt} = \frac{du_4}{dt}$.



Mallory Attacks Healing Variable: Meta Operator 2 Fails

$\eta_2(t)$ attacks signal variable u_2. $\eta_3(t)$ attacks healing variable u_4.



$\eta_i(t) = \chi(t, \frac{33}{2}, \frac{1}{2}, \delta_i, 5, \frac{3}{2})$, where $\delta_2 = \frac{1}{3}$ and $\delta_3 = 1$.

$\chi(t, l, f, \delta, k, \mathcal{A}) = \mathcal{A} * g(t, l, \delta, k) * h(t, l, f)$.
$g(t, l, \delta, k) = \tanh(k(t - l)) + \tanh(-k(t - l + \delta))$.
$h(t, l, f) = \sin\left(2\pi f(t - l)\right)$.

Decentralize Roles of Signal & Healing Variables

Healing variable is a single point of failure of meta operator 2.

Use six variables $u_1, \ldots, u_6$. Decentralize roles of variables u_i.

Meta Equations: $\omega_1(0) = \omega_2(0) = \omega_3(0) = 0.$

$$\frac{d\omega_1}{dt} = \frac{du_4}{dt} - \frac{du_2}{dt}. \quad \frac{d\omega_2}{dt} = \frac{du_6}{dt} - \frac{du_4}{dt}. \quad \frac{d\omega_3}{dt} = \frac{du_2}{dt} - \frac{du_6}{dt}.$$

Meta Operator 5:

$$\text{if} \quad |\omega_1(s_1)| \geq \theta \quad \text{and} \quad |\omega_3(s_3)| \geq \theta \quad \text{set} \quad \frac{du_2}{dt} = \frac{1}{2}\Big(\frac{du_4}{dt} + \frac{du_6}{dt}\Big).$$

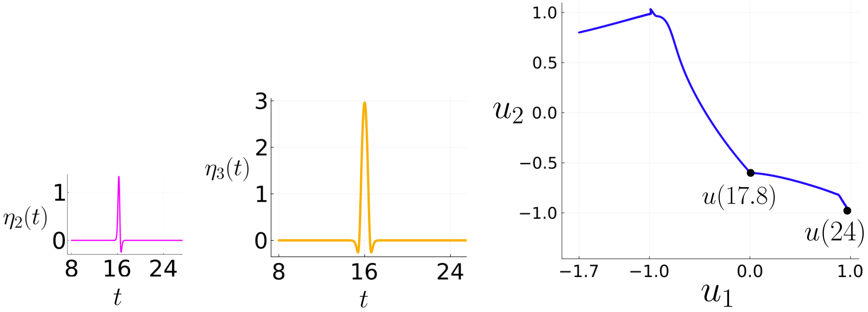
$$\text{if} \quad |\omega_1(s_1)| \geq \theta \quad \text{and} \quad |\omega_2(s_2)| \geq \theta \quad \text{set} \quad \frac{du_4}{dt} = \frac{1}{2}\Big(\frac{du_2}{dt} + \frac{du_6}{dt}\Big).$$

$$\text{if} \quad |\omega_2(s_2)| \geq \theta \quad \text{and} \quad |\omega_3(s_3)| \geq \theta \quad \text{set} \quad \frac{du_6}{dt} = \frac{1}{2}\Big(\frac{du_2}{dt} + \frac{du_4}{dt}\Big).$$

Meta Operator 5 Succeeds

Succeeds with same noise pulses η_2, η_3. (Meta operator 2 fails.)

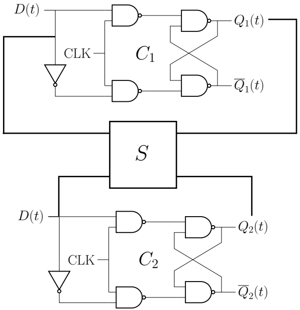
Noise pulses attack u_2 and u_4, respectively.



Hardware Gedankexperiment

Tests feasibility of building meta operator 2.

C_1 and C_2 are D flip-flop circuits. S is a self-modifiable circuit.



Circuit S computes $\frac{d\omega_1}{dt} = \frac{du_3}{dt} - \frac{du_1}{dt}$. $\frac{d\omega_2}{dt} = \frac{du_4}{dt} - \frac{du_2}{dt}$.

if $|\omega_1(s_1)| \geq \theta_1$ or $|\omega_2(s_2)| \geq \theta_2$ circuit S self-modifies circuit C_1.

Research Summary

- A *D* flip-flop differential equations model was used.
- A noise attack can disrupt a flip-flop orbit.
- Analogous to error codes, additional (healing) variables, meta variables, meta operators and self-modifiable differential equations can help ameliorate a noise attack.
- Signal functionality and healing should be decentralized over standard and meta variables.
- Outlined a hardware design: tests meta operator 2's feasibility.

Research Questions

- Can a hardware flip-flop self-modify to hinder noise attacks?
- Can a chaotic attractor decentralize signal and healing among multiple variables?
- Can bifurcation theory provide insight on how to design new meta operators?
- Can quantum entanglement help self-modify a quantum dynamical system?