~~Electrical Noise~~ Chemical Chaos based Truly Random Number Generator

Raja Vinay Chandra
Souvik Dutta
Saumya Dhawan

Guidance: Prof. Pradeep Sarin

November 16, 2011

1 Introduction

1.1 Random Numbers

The Oxford English Dictionary defines 'random' as "Having no definite aim or purpose; not sent or guided in a particular direction; made, done, occurring, etc., without method or conscious choice; haphazard." A random number sequence that is haphazard, and impossible to predict. A random number generator seeks to generate a sequence of random numbers utilizing some physical process, or in the case of a computational algorithm, atleast fake them. Random numbers find widespread use in gambling, algorithm testing, cryptography, and even art!. In fact, the growing number of casinos, lotteries and slot machines makes it a billion dollar industry.

1.2 True v/s Pseudo-Random Numbers

Two distinct principles in random number generation are the use of physical processes and computer algorithms. As the title suggests, numbers generated using deterministic computer algorithms are not "true" random numbers since it's output is traceable and hence unsafe. In this project, we had intended to generate true random numbers by utilizing a physical process that was indeterministic.

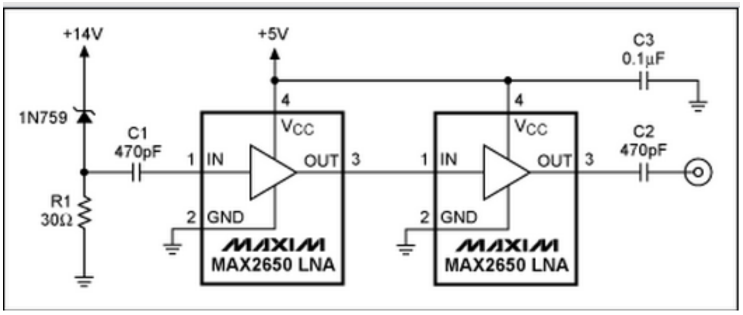
2 Initial attempts

Our initial attempts for a physical system were mainly focussed towards electrical systems which produced noise or showed appreciable amounts of non-linearity. Two main contenders were Avalanche Noise across a p-n junction and Chua's circuit, often considered to be the paradigm for Chaos.

2.1 Avalanche Noise

Avalanche noise is noise produced when a junction diode near the breakdown region. In this region, additional carriers cause irregular current flows, which if properly tapped could give random signals, i.e. noise.

For this purpose, we borrowed a noise generating circuit from the Internet that was shown to give good results.

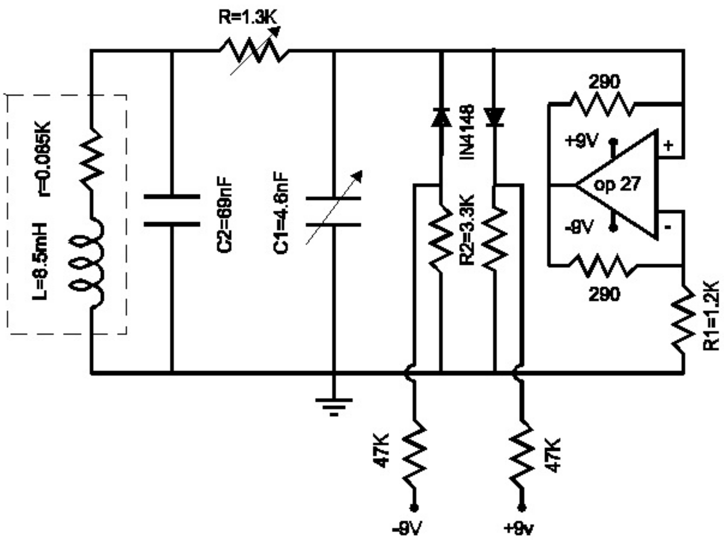


However, inspite of trying multiple times at multiple places(Whenever electronics is involved, space no longer remains isotropic), we could not get appreciable results inspite of multiple amplifications. We had even tried gradual amplification using 4 amplifiers in series.

We suspect there was too much interference with our apparatus, (a breadboard and subsequently a scrapboard) from external fields as well as with the components that were involved that might have coupled with our noise to give sort of a weighted signal that amounted to nothing for our purpose[1].

2.2 Chua's circuit

We tried implementing this circuit but could not match the component values successfully to bring about the chaos described in literature. The study of it, though, was quite interesting. We also came into conversations with a couple of Prof. Punit's students.



[1]On retrospect, we could have tried enclosing the entire apparatus in a metal box and used a compact PCB(but costly)

3 Chaos From a Chemical System

Chemical Noise remains an interesting phenomena, more so because of its rarity. *Chemical Oscillators* are probably more common than Chaos. The system we selected (known as **Mercury Beating Heart** in popular literature) was tried on the most unsure footing. Even after having observed random signals in the initial stages, the Noise (if it were) hardly persisted. But before delving into the functioning, the phenomenon is worth a description.

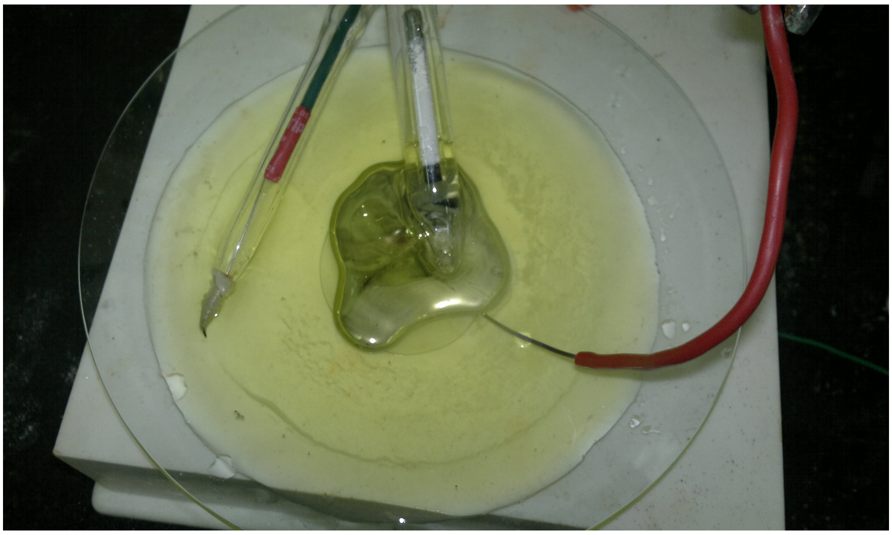
3.1 The Setup:

The Mercury Heartbeat experiment has been performed(Kuhne, Lippmann), and has some accessible literature on the same on the Web. The fundamental idea behind the experiment is significant amount of difference in **Surface Tension** between **Elemental Mercury** and **Mercury (II) ions**. 6 ml of Mercury is poured carefully on a watch glass of radius (approx.) 7-8 cm. A standardized solution of $Ce(SO_4)_2$ is titrated against a 6 M Solution of (Conc.) H_2SO_4. Approx 15 ml of this $Ce(SO_4)_2$ solution is poured on the Mercury blob, so as to just cover it. A few drops of 6 M H_2SO_4 is added to the solution.

The mercury drop, an iron nail, and the acidic solution of acidic $Ce(SO_4)_2$ constitute a galvanic cell in which the mercury serves as the cathode and the iron serves as the anode. There is a voltage difference between the iron and mercury electrodes. During the time when there is no electrical connection between the mercury and the iron, $Ce(SO_4)_2$ oxidizes Hg (elemental) to Hg_2SO_4, which forms a layer on the mercury surface. This surface layer reduces the surface tension of the liquid mercury, allowing the mercury drop to flatten. Eventually the mercury contacts the iron nail and the cell is short circuited. Transfer of electrons from the iron to the mercury (and thence to the Hg_2SO_4) surface film reduces the Hg_2SO_4 back to metallic Hg. This increases the surface tension of the mercury and the drop becomes rounder, causing it to recede from the nail and break the circuit. Then the surface film builds up again as a result of oxidation of mercury by the $Ce(SO_4)_2$. This keeps happening until we reach the exhaustion of the ***Limiting Reagent***.

3.2 The Behaviour:

The reaction slowly runs down over a period of a few hours, until all oscillatory activity eventually ceases. During this period the dynamics slowly evolves, showing qualitatively different forms of oscillations. These oscillations display different modes of oscillations with geometric structures similar to heart, circle, pentagon, hexagon, and 8- and 16-pointed stars. As time proceeds, limit-cycle oscillations of period-1, period-3, and period-2 appear successively. However, these oscillations are damped and could be interpreted in terms of a subcritical ***Hopf Bifurcation***. Alternatively, it could also be seen as a ***Period doubling way to Chaos***, the exact process we weren't very sure of.



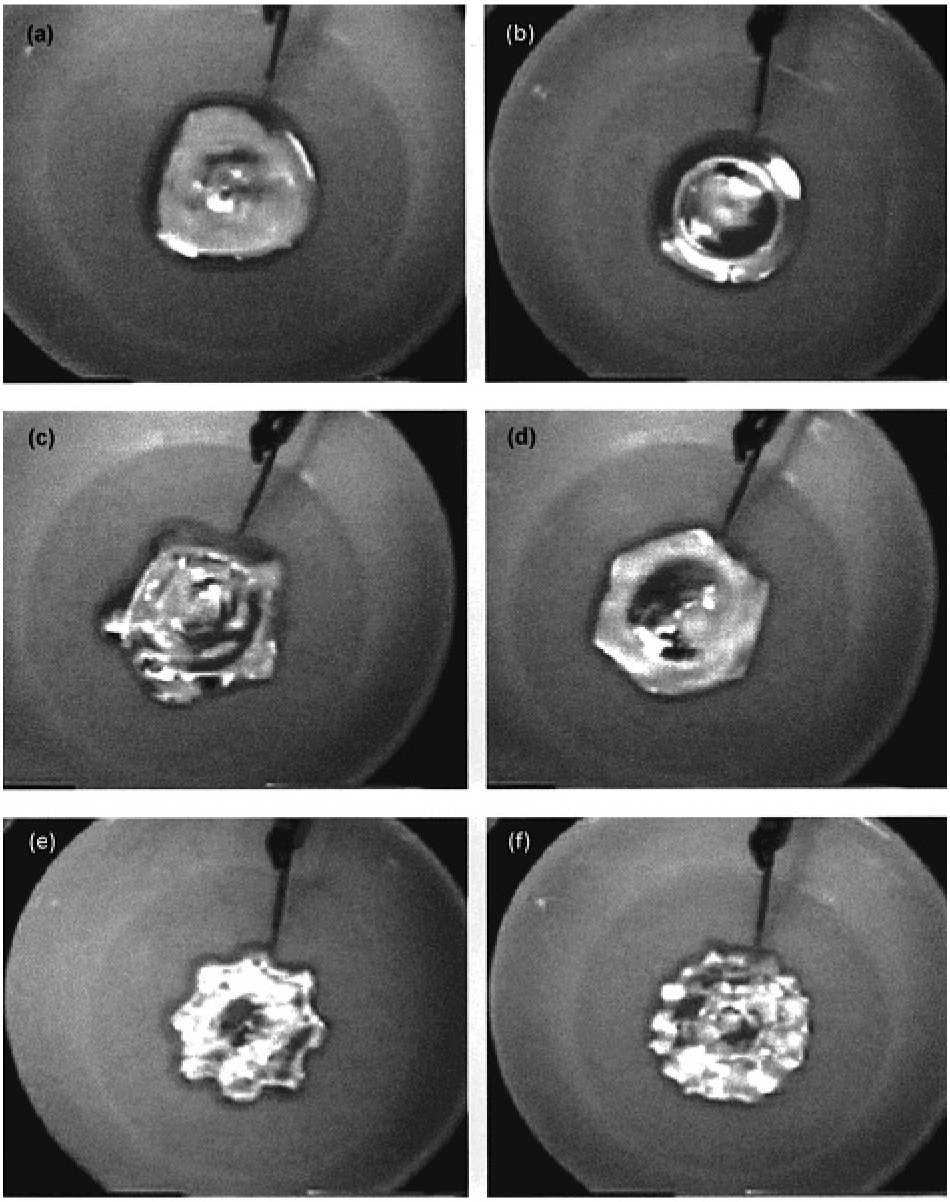
3.3 The Chemical Reaction

$2[Ce^{IV}(SO_4)_3]^{2-} + 2Hg^0 \leftrightharpoons Hg_2^{2+} + 2[Ce^{III}(SO_4)]^{+} + 4[SO_4]^{2-}$
$Fe^0 + Hg_2^{2+} \leftrightharpoons Fe^{2+}\ (aq) + 2Hg^0$

As shown, Hg gets oxidized and reduced once every "heartbeat".

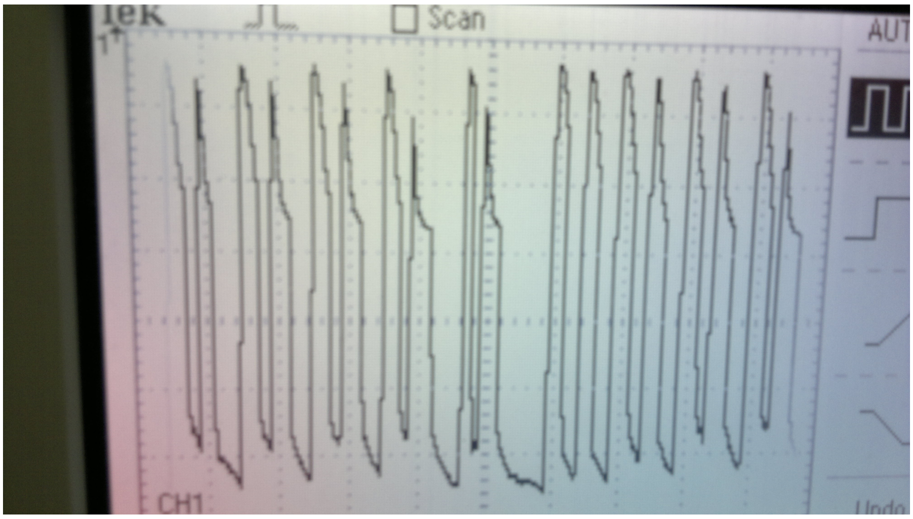
3.4 Generating Random Numbers

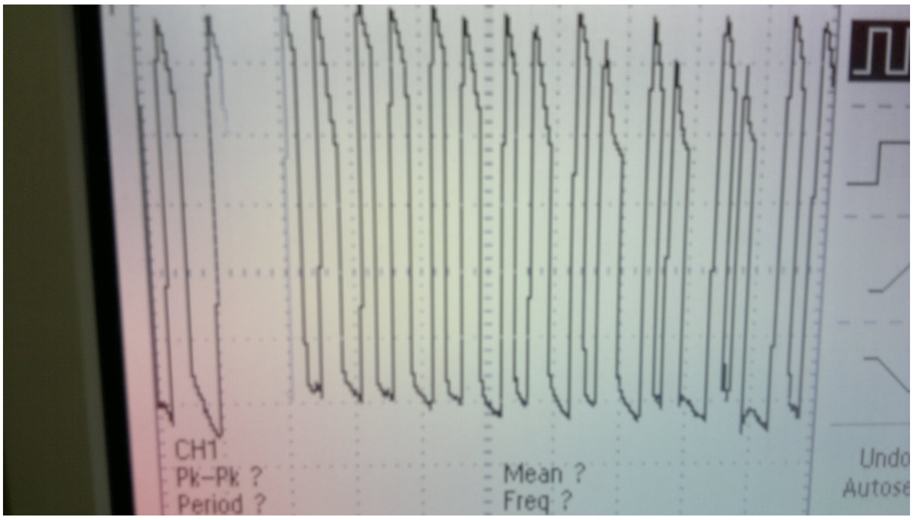
The system (probably) develops by the period doubling route to chaos. The following images would demonstrate the shapes seen. The biggest challenge was to ***prolong*** the duration of chaos. Initially, with low $Ce(SO_4)_2$ concentrations, the shapes weren't very distinct, and with higher concentrations, Chaos was never apparent. At an optimum $Ce(SO_4)_2$, H_2SO_4 concentration, the shapes were good, and Potential fluctuations (measured between the Acidic solution and Hg) was measurable by the Arduino ADC.



3.5 On the Oscilloscope

To make sure we were making measurements in the ***Chaotic Regime***, we checked the Analog Signals on the Oscilloscope. Here is what we observed.





On inquiring of Prof. Punit, he confirmed that what we were seeing was indeed chaos.

4 Arduino code

The ADC received signals in the form of Analog Voltage between approx. 0 to 780 mV. This was sufficient to generate a decent Digital counterpart. Here is the code which made the Arduino sample the incoming signals continuously but return a random value on demand (conveyed by entering ”1”).

```
int incomingByte = 0; // for incoming serial data
int analogPin = 3;     // potentiometer wiper (middle terminal)
                       //connected to analog pin 3
                       // outside leads to ground and +5V
int val = 0;           // variable to store the value read

void setup() {
Serial.begin(9600); // opens serial port, sets data rate to 9600 bps
}
void loop()
{
  val = analogRead(analogPin);    // read the input pin

// send data only when you receive data:
if (Serial.available() > 0) {
// read the incoming byte:
incomingByte = Serial.read();
if(incomingByte==49)
{
  Serial.println(val%10+1);     //prints a random number between 1 and 10



// say what you got:
//Serial.print("I received: ");
//Serial.println(incomingByte, DEC);


  Serial.println(val);             // debug value
}
}
```

5 Conclusion and Possible Uses

Given the need to generate truly random numbers, this experiment tries to approach the problem with a fresh outlook. Inspite of having the shortcomings of portability and reproduction, it does show how to produce Random numbers with a completely non-deterministic manner. They then,can be used for anything, ranging from Gambling to Statistics. This last image shows the variations of the obtained values versus time.