

Lecture 4

“Noise” as a random number generator

Plan of the Lecture

Extracting randomness from physical noise

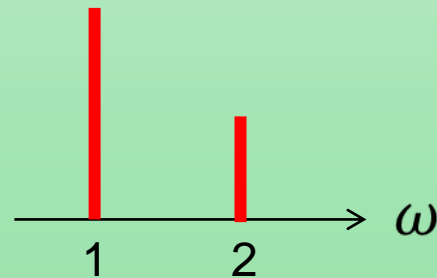
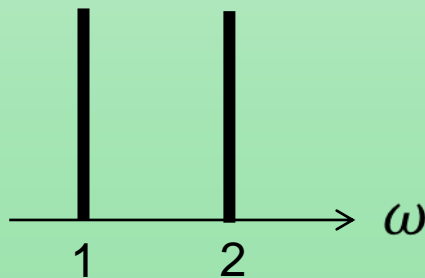
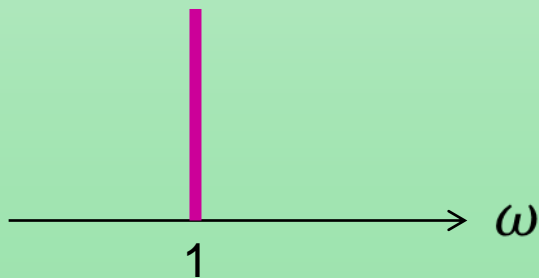
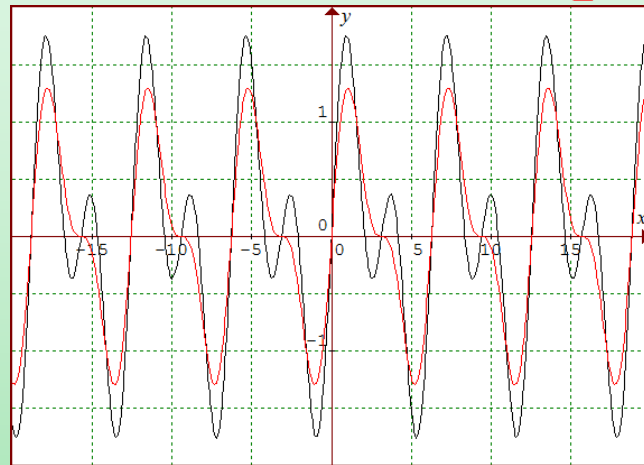
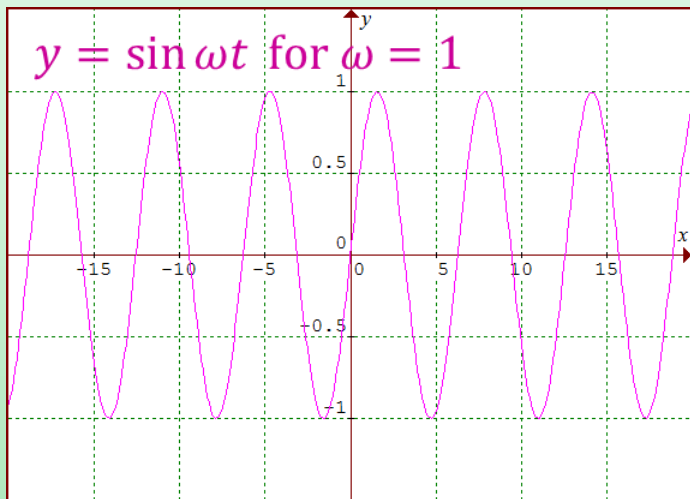
- 1 Technical definition of noise
- 2-3 Thermal noise
- 4 Randomness from noise

MATHEMATICS OF “NOISE”

Many frequencies

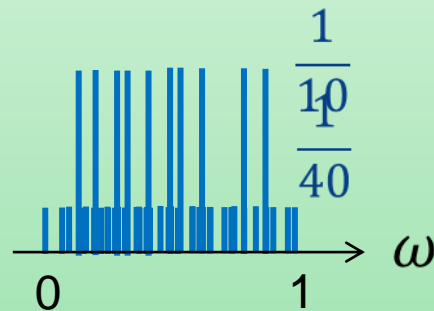
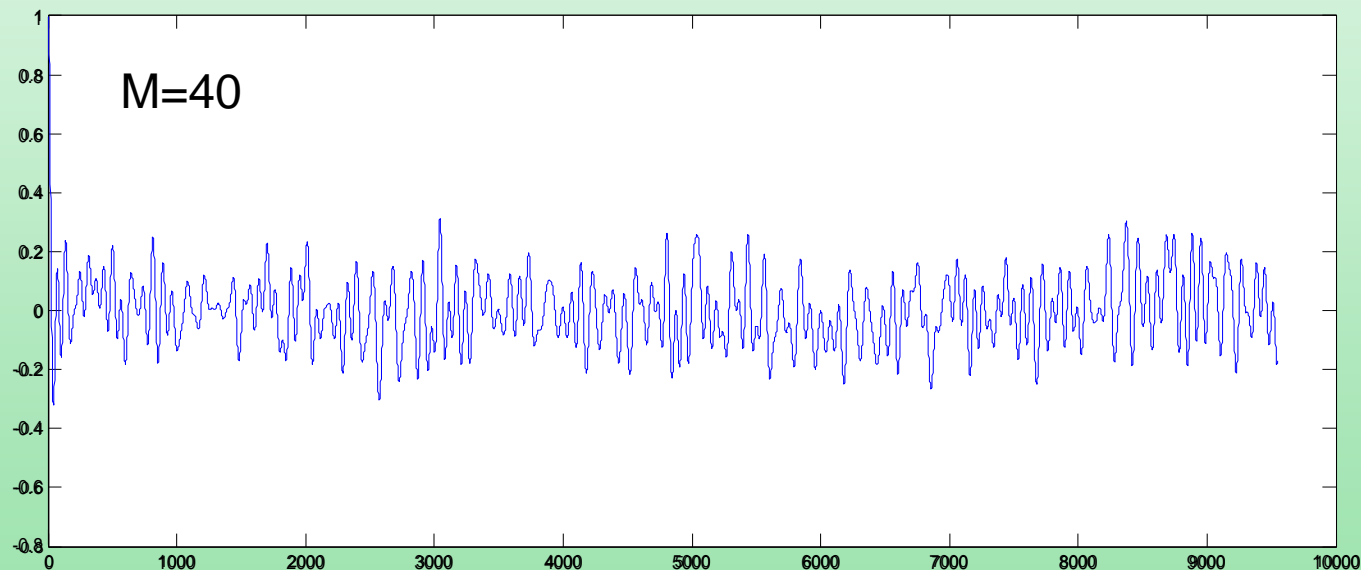
Frequency spectra

$$y = \sin \omega t + \sin 2\omega t \quad y = \sin \omega t + \frac{1}{2} \sin 2\omega t$$



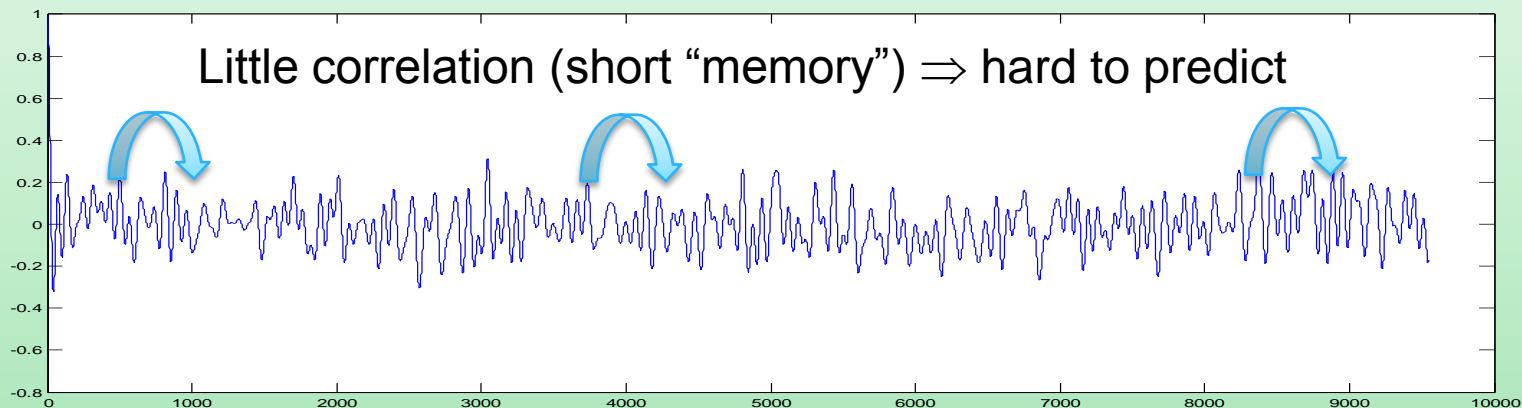
Adding frequencies

$$f(x) = \frac{1}{M} \sum_{k=1}^M \cos(\omega_k t)$$

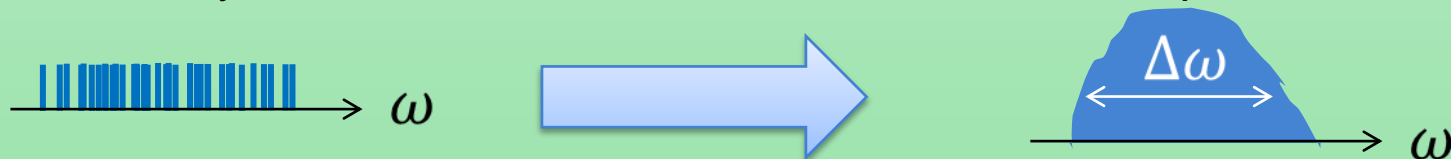


Noise

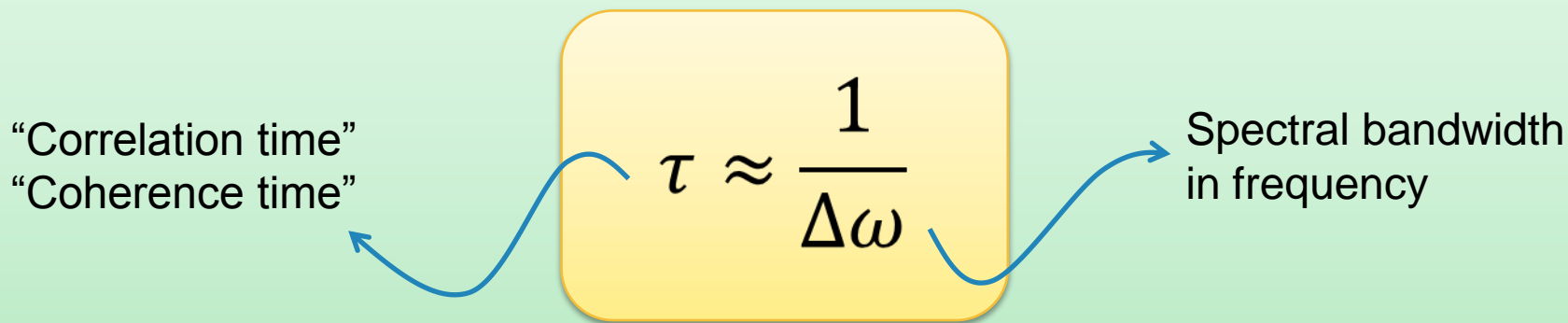
More frequencies in the spectrum \Rightarrow more noisy signal



In fact, many natural source of noise have a continuous spectrum:



Spectral bandwidth vs. memory time



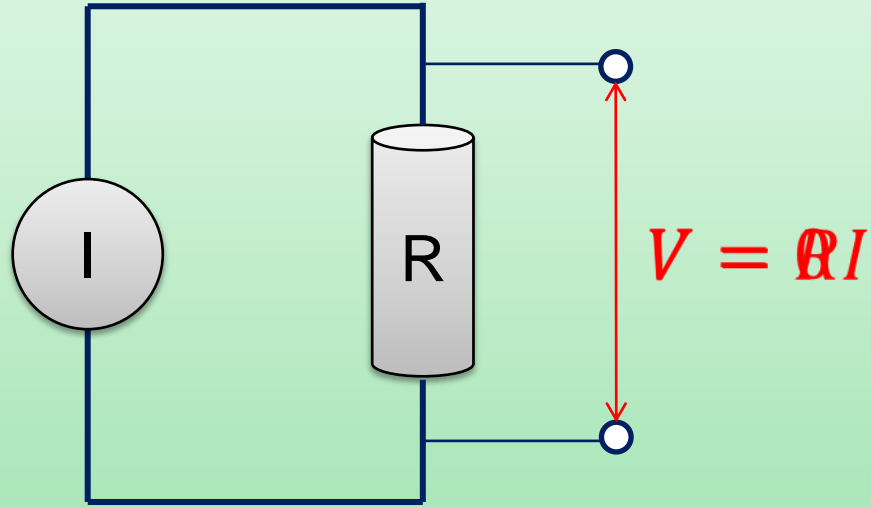
Not to be confused with the relation $\Delta t \Delta\omega \geq 1$ for Fourier transforms: there, Δt is the temporal length of the signal (e.g. the width of a pulse).

- Obviously $\tau \leq \Delta t$: once the signal is finished, it certainly cannot encode any more memory of its values at previous times.
- A signal for which $\Delta t = \tau$ is called “Fourier-limited”.

THERMAL NOISE

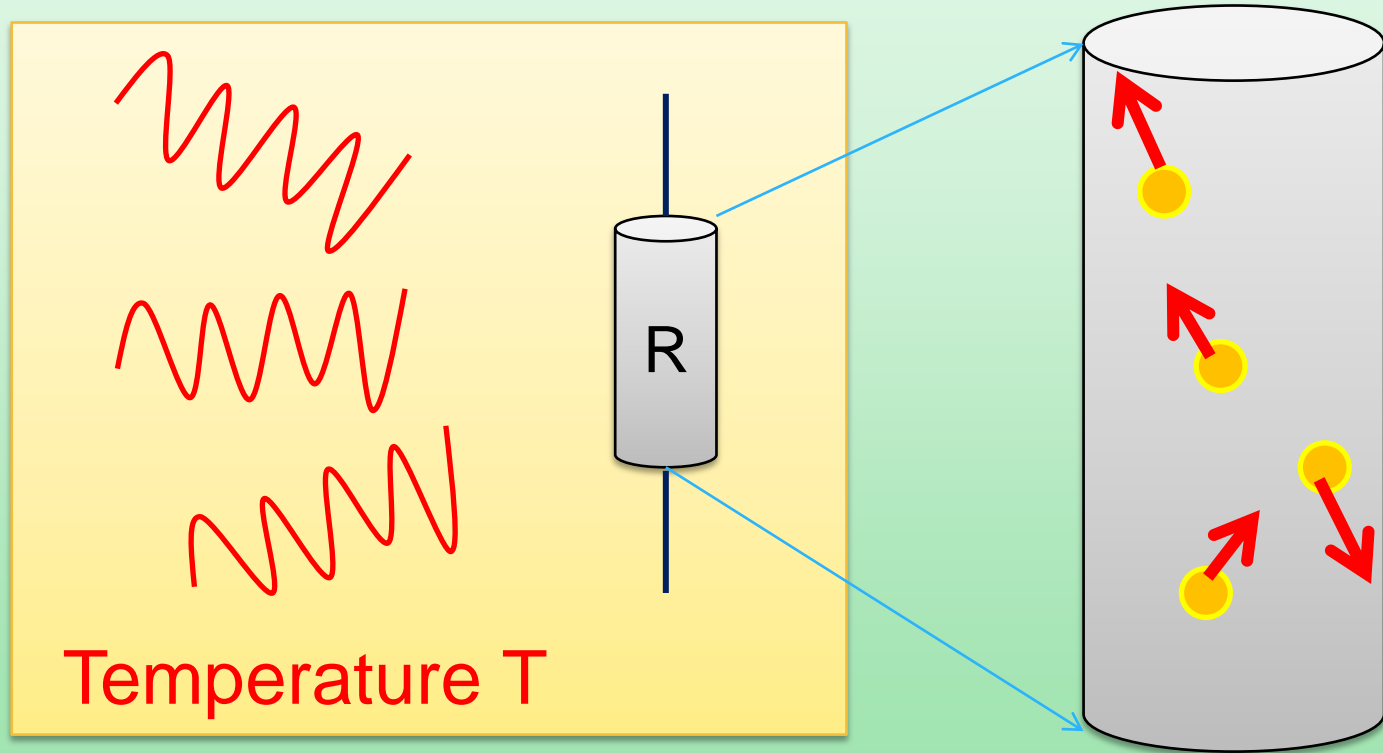
Theory

A resistor

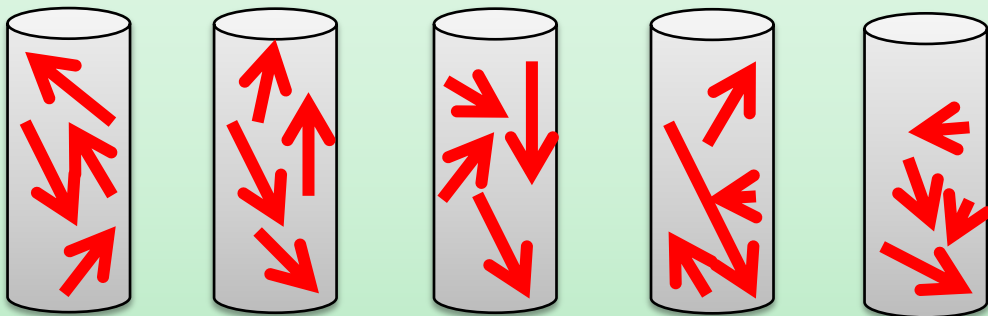


Really zero?

Contact with a thermal bath



Thermal noise



$V=RI=0$ is
the average

Thermal
fluctuations

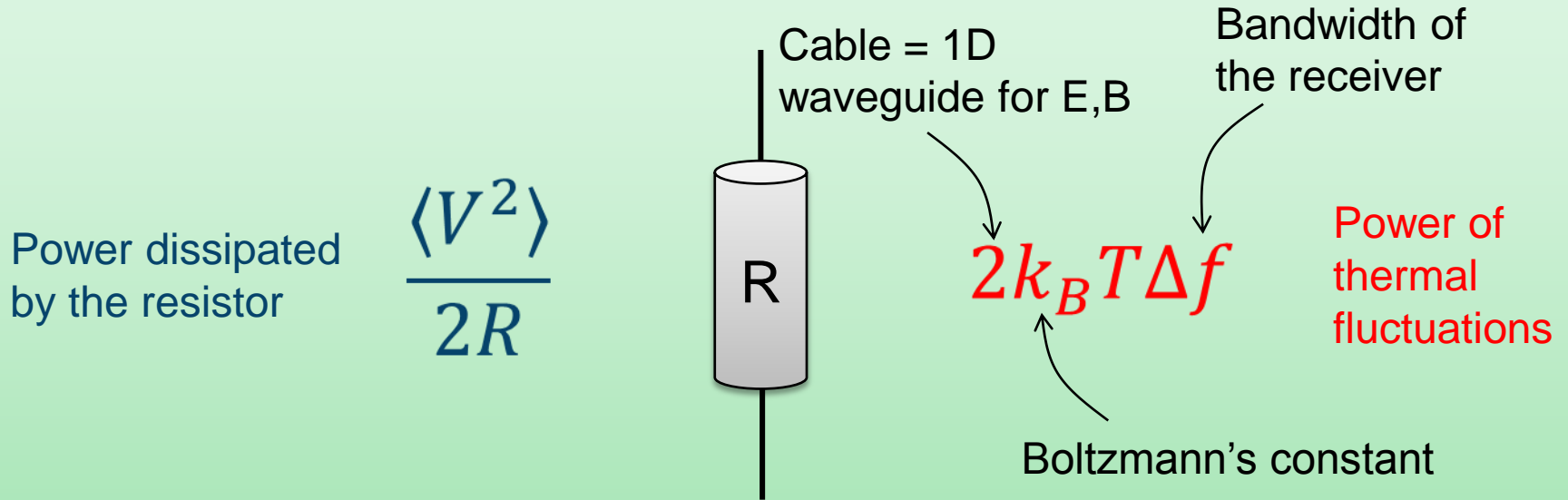
Johnson-Nyquist noise

- The thermal noise of the resistor is named after John Johnson, who reported it, and Harry Nyquist, who did the theoretical description (Bell Labs, 1932)
- From Johnson's paper:

“The mean-square potential fluctuation over the conductor is *proportional* to the electrical resistance and the absolute temperature of the conductor. It is *independent* of the size, shape or material of the conductor.”

That is: $\langle V^2 \rangle \propto R T$

The formula



At equilibrium, they must be equal \Rightarrow

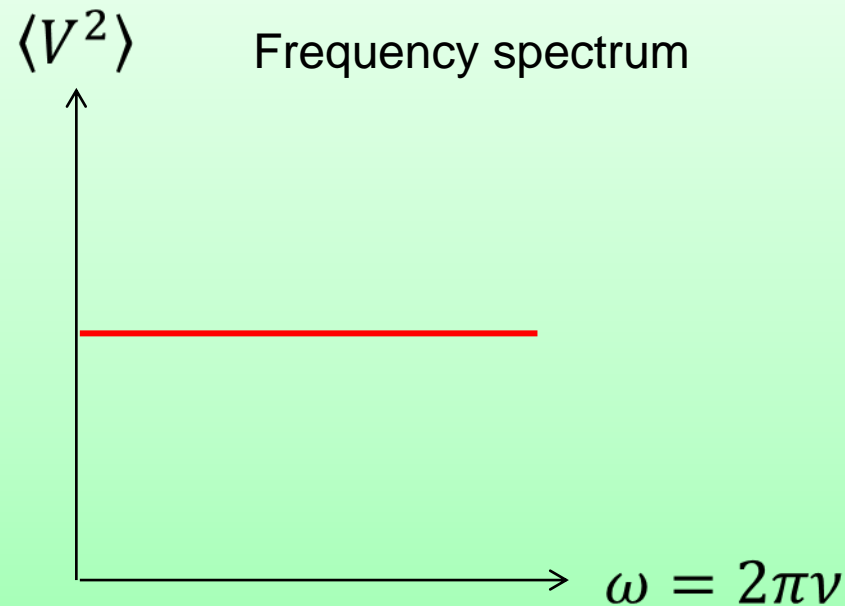
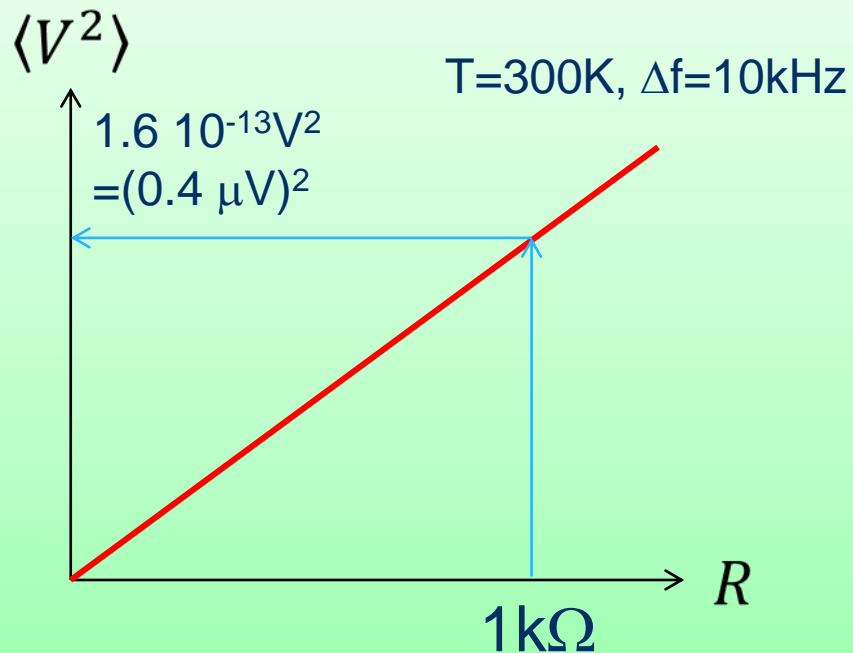
$$\langle V^2 \rangle = 4k_B T R \Delta f$$

More rigorous derivation

- For each frequency interval $d\nu$ it holds: $d\left(\frac{V^2}{2R}\right) = \bar{E}(\nu)2d\nu$
where $\bar{E}(\nu) = \frac{h\nu}{\exp\left(\frac{h\nu}{k_B T}\right) - 1}$ is the Planck formula and $2d\nu$ is the density of states for the field in 1D (two polarizations).
- For frequencies of thermal radiation, one can safely replace $\bar{E}(\nu) = k_B T$. Then the r.h.s. becomes independent of the frequency and one can integrate to obtain the formula give before.
- Without Planck: e-m field energy is $E^2 + B^2$ and there are two polarizations, so in 1D we get $4 \times \left(\frac{k_B T}{2}\right)$.

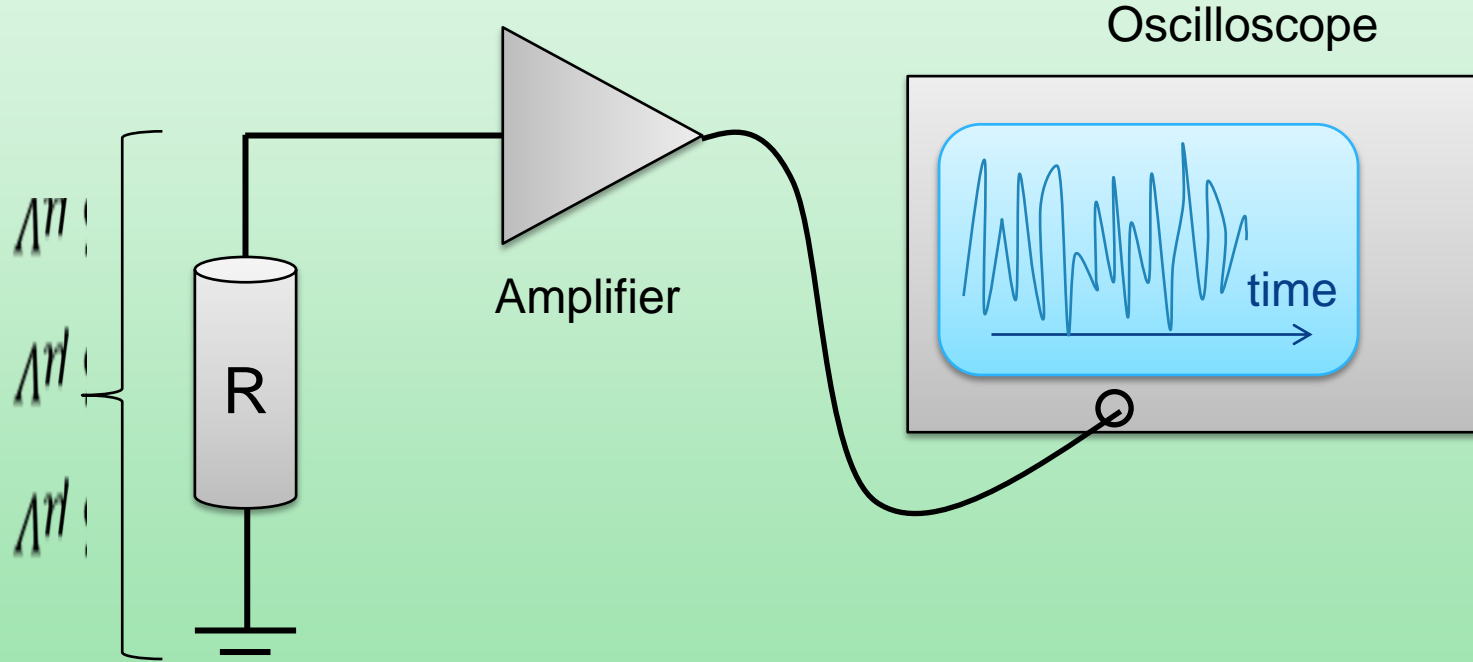
Predictions in graphs

$$\langle V^2 \rangle = 4k_B T R \Delta f$$

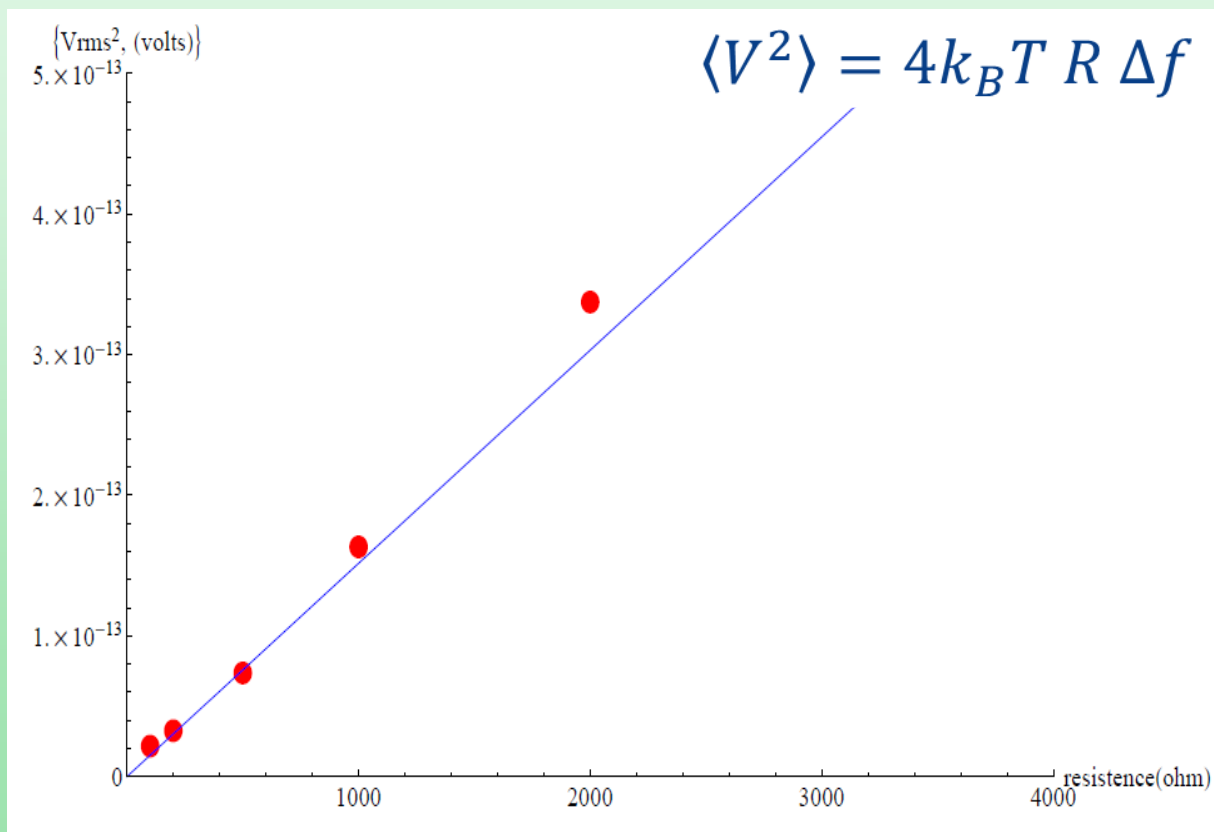


NOISE IN THE LAB

Devices




Observation



RANDOMNESS FROM NOISE

Statistics of noise

- We know: average $\langle V \rangle = 0$, fluctuations $\Delta V = \sqrt{\langle V^2 \rangle}$.
- For randomness extraction, we need the full distribution $P(V)$ in order to compute entropies.



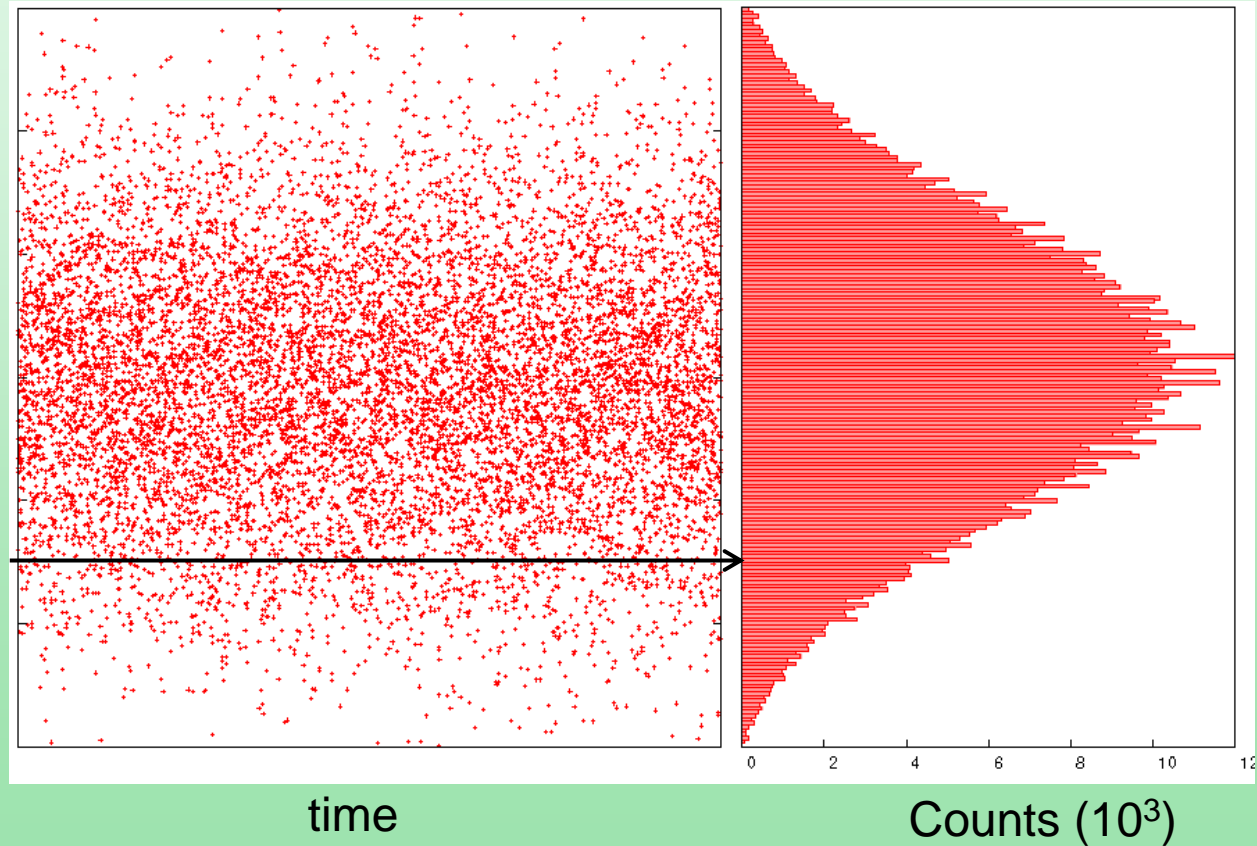
The observed distribution is enough, because we have a **controlled source of noise**:

- we checked that the noise is the one expected for thermal noise
- we trust physics that it is a phenomenon too complex to predict.

One could put up an antenna and capture unknown signals, that may look random to us. But they may not be random for others, or may have unwanted structure in them.

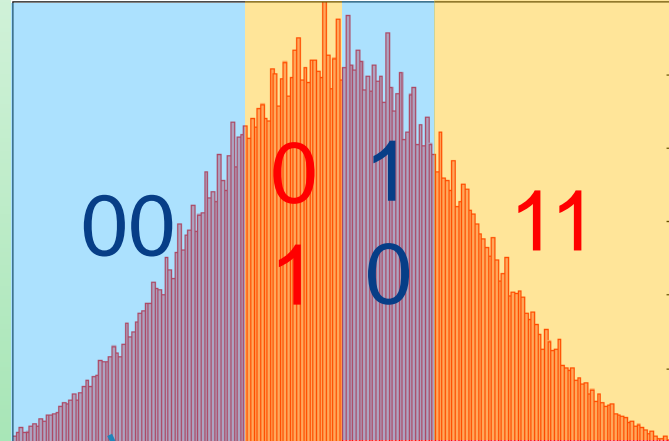
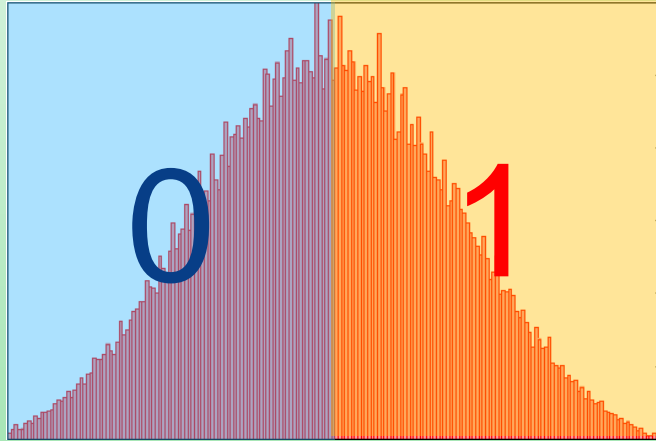
Observed distribution

$R=1\text{k}\Omega$
 $T=300\text{K}$



Possible processing (1)

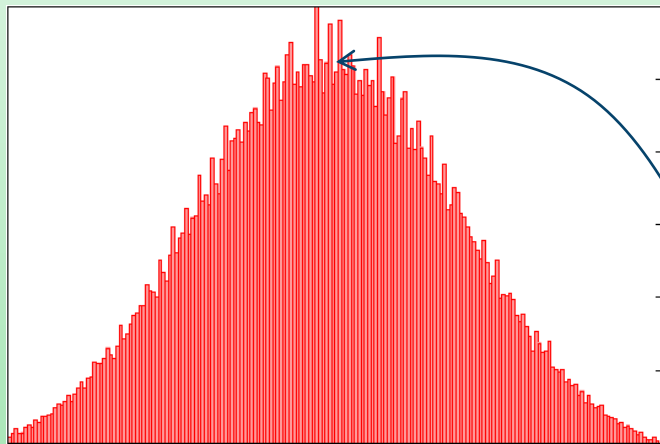
Try to get directly fair coin sequences out of it



More than one bit \Rightarrow need to adapt carefully the intervals in order for each sequence to have the same probability

Possible processing (2)

Estimate $P(V)$, then use extractors



This analog conversion has 256 channels



$\{P(1), P(2), \dots, P(256)\}$

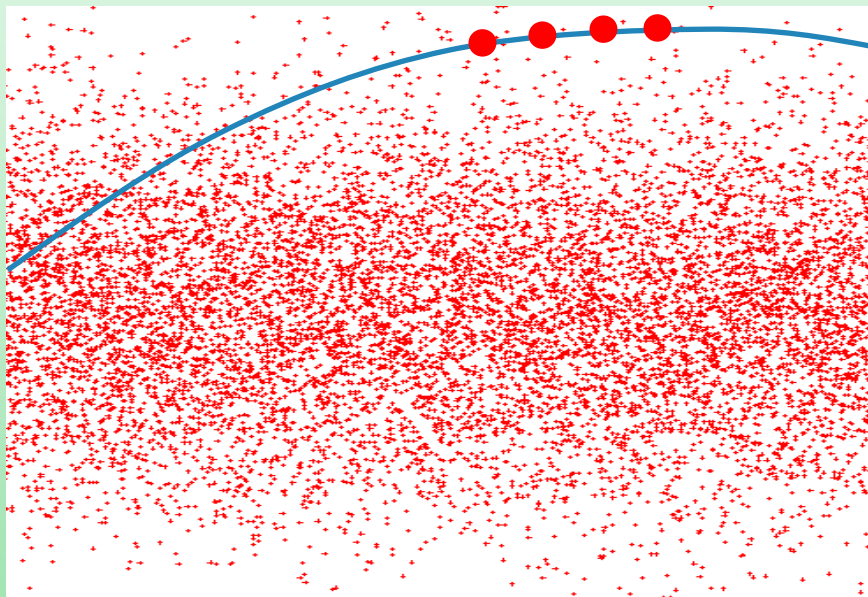
$$P_{guess} \approx P(128) = P(V = 0)$$

$$\approx 0.01 \Rightarrow H_{min} \approx 6.5 \text{ bits/signal}$$

Remark: for a trusted source, one can be less conservative and compute randomness from the average (“Shannon”) entropy.

Correlations from finite bandwidth

Previously we assumed that each value of V is independent of the others, but:



- High frequency cutoff \Rightarrow values within $\tau = \frac{1}{\Delta\omega} \approx \frac{1}{\omega_{max}}$ are correlated
- Low frequency cutoff \Rightarrow long sequences of large amplitudes become less probable than they should

As we know, no problem in principle: just estimate P of each sequence, then compute H_{min} . But in practice, this is not feasible.

Suggested Readings

Wikipedia pages:

- http://en.wikipedia.org/wiki/Hardware_random_number_generator

Summary of Lecture 4

Extracting randomness from physical noise

- Noise = large spectrum of frequencies
- Thermal noise
- Extracting randomness, effects of correlations