Guesswork is not a substitute for Entropy

David Malone and Wayne Sullivan

Measuring Randomness

* simple measurement of uncertainty: a program that reads n bits of random state can only have 2^n outcomes.
* Lotto: 42!/6!36! = 5245786 (23 bits)
* Shuffling Card: 52! = 8.0658×10^{67} (29 bits)
* Shuffling Votes: 1000000! (20 million bit = 1.25MB)

Entropy Measuring Uncertainty

* Source produces symbol a with prob p_a.
* Entropy $h(p) := -\Sigma p_a \log(p_a)$
* Shannon: h(p) is average number of bit required to encode long message.
* Nice properties: adds for independent.
* Often thought of as uncertainty.

Guessing and Cryptography

* Encryption uses algorithm and key.
* Algorithms usually carefully chosen.
* Easier to attack key?
* Brute Force Attack vs. Dictionary Attack.
* Not just people - need to seed PRNGs.

Entropy and Guessing

* Does Shannon's Entropy capture hard to guessness?
* sci.crypt FAQ:

  We can measure how bad a key distribution is by calculating its entropy. This number E is the number of ``real bits of information'' of the key: a cryptanalyst will typically happen across the key within 2^E guesses.

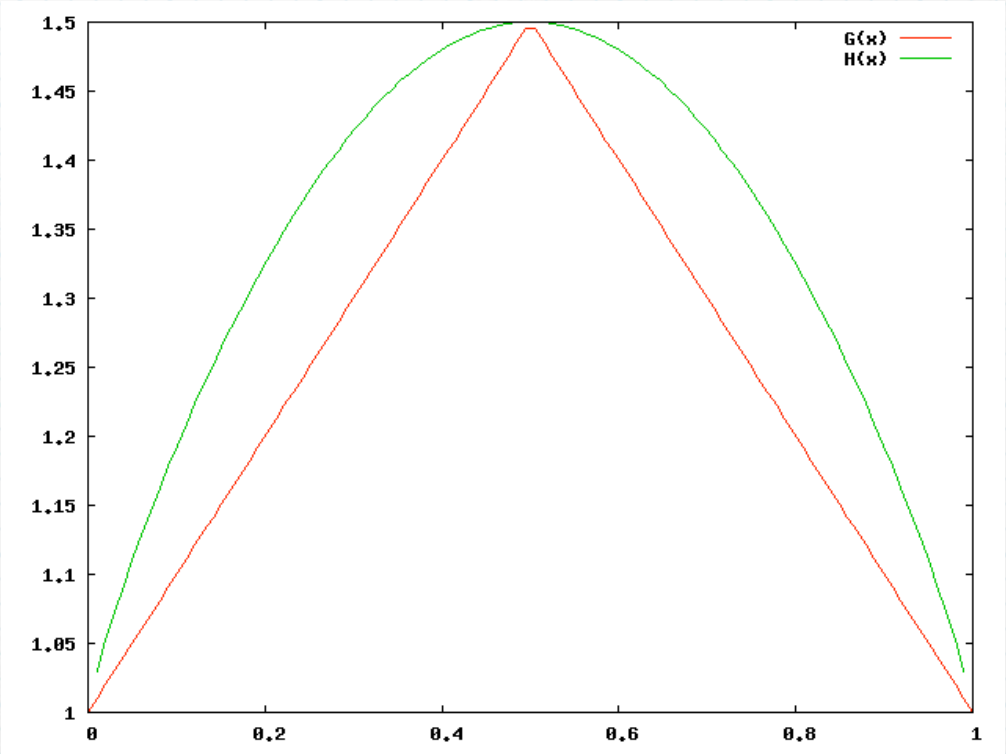
* No proof offered - can we check?

Guesswork

* Quickest way to guess is from most to least likely.
* Sort p_i so that p_1 is most likely then p_2, ...
* Mean number of guesses: $G(p) := \Sigma i\ p_i$
* Compare to $H(p) = (2^{h(p)} + 1)/2$.

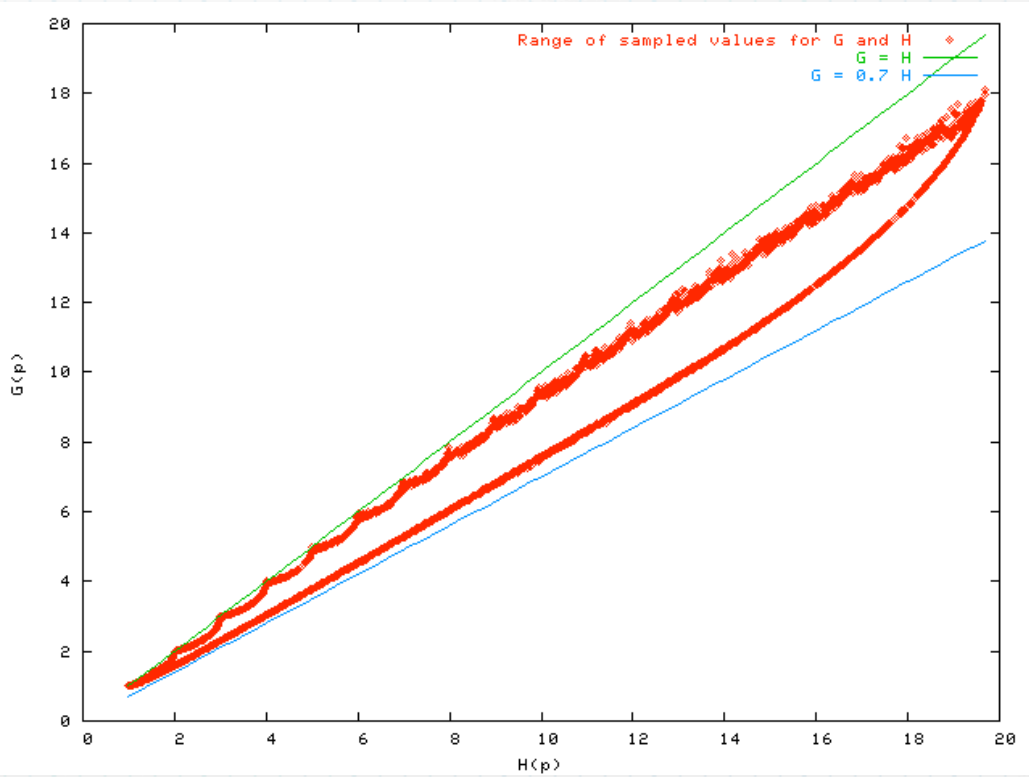
Single Random Bit

- Choose single random bit with some prob.
- Compare Entropy H and Guesswork G.
- Similar, not same.
- Note effect of sorting.



Multi-Symbol Sources

- Simulate source with up to 20 symbols.
- Sample 1000000 distributions for each number.
- 0.7 H(p) ≤ G(p) ≤ H(p)?
- No! (Massey, Arikan, ...)



Other measures

* Guesswork is related to Réyni entropy.
* Other measures of guessability
* work-factor (give up after most of prob)
* distance from uniform
* (RFC 4086) min-Entropy

Moral

* Don't always believe simulations.
* Decide what you want your randomness for, choose the right measure.
* Crypto guys didn't but got lucky.
* Arcane mathematical abstractions get applied sooner or later.