1. Shannon entropy vs. Kolmogorov complexity

(K) $\forall x \exists y\ \Phi(C(x_1), C(y_1), C(x_1, y_1), \dots)$.

Here:
x, y are tuples of strings,
$x = (x_1, \dots, x_k)$, $y = (y_1, \dots, x_m)$.
Φ is quantifier free monotone combination of linear inequalities of the form
$aC(x_1) + bC(y_1) + dC(x_1, y_1) + \dots \leq o(n)$,
$n = \max\{C(x), C(y)\}$.

(H) $\forall \alpha \exists \beta\ \Phi(H(\alpha_1), H(\beta_1), H(\alpha_1, \beta_1), \dots)$.

(SH) $\forall \alpha \forall n \exists \beta\ \Phi(H(\alpha_1^n), H(\beta_1), H(\alpha_1^n, \beta_1), \dots)$.

Examples

1. Extractability of mutual information: $\forall x \forall y \exists z$
$[C(z) = I(x : y) + o(n) \ \wedge \ C(z|x) = o(n)$
$\wedge \ C(z|y) = o(n)]$.

2. Muchnik's theorem $\forall x \forall y \exists z$
$[C(z) \leq C(y|x) + o(n)$
$\wedge \ C(y|x, z) = o(n) \ \wedge \ C(z|y) = o(n)]$.

Problems

Obviosly (H) $\Rightarrow$ (SH).

Is it true that (H) $\Rightarrow$ (K) ?

Is it true that (K) $\Rightarrow$ (SH) ?

What is known

(K) $\not\Rightarrow$ (H):

$$\forall x \forall y \exists z \; C(z) + C(y|z,x) + C(x|z,y) \leq \max\{C(x|y), C(y|x)\} + O(\log n)$$

(SH) $\not\Rightarrow$ (K):

$$\forall \xi, \eta \; \forall \boldsymbol{n} \; \exists \beta$$

$$[H(\beta) \leq \frac{H(\xi^n) + H(\eta^n)}{2} + O(1),$$

$$H(\xi^n|\beta) \leq \frac{H(\xi^n|\eta^n)}{2} + O(1),$$

$$H(\eta^n|\beta) \leq \frac{H(\eta^n|\xi^n)}{2} + O(1)].$$

2. Komogorov complexity and cryptography

$I(p : y) = C(y) - C(y|p)$

$D(x, y) := \max\{C(y|p) \mid p \text{ is a program for } y \text{ given } x\}$

Observation: $D(x, y) \leq \min\{C(x), C(y)\}$.

Theorem (Muchnik)

$D(x, y) = \min\{C(x), C(y)\}$.

Generalization

The eavesdropper has some a priori information s.

$D(x, y|s) := \max\{C(y|p, s) \mid$
p is a program for y given $x\}$

Theorem (Muchnik)

$D(x, y|s) = \min\{C(x|s), C(y|s)\}.$

Minor point: the length program p in the theorem is exponential in n!

Problems

1. Is it true: for all x, y, s there is p, a program for y given x, with $C(p) = \text{poly}(n)$ and $C(y|p, s) = \min\{C(x|s), C(y|s)\} + o(n)$?

2. Assume that the eavesdropper needs information about yet another string t. What can be said about $\max\{C(t|p, s) \mid p \text{ is a program for } y \text{ given } x\}$? Can this value be expressed through the complexity profile of x, y, s, t?

3. Maximizing mutual information by relativization

Assume that x, y are given. What can be said about $\max\{I(x : y|z) \mid z \in \{0,1\}^*\}$? Is it true that it equals $\min\{C(x), C(y)\}$?

(Suleikin) A similar question for Shannon entropy: how to find for given joint distribution of random variables A, B the value $\max_X I(A : B|X)$? Is it true that the maximum is always attained for a random variable X with at most $|A| \cdot |B|$ outcomes?