Error correcting code and computability theory

Benoit Monin

LACL
Université Paris-Est Créteil

30 June 2016

Coarse computability

Given a set $A \subseteq \mathbb{N}$. How close is A to being computable ?

A recent paradigm : A is coarsely computable. This means there is a computable set R such that the asymptotic density of

$$\{n\colon\ A(n) = R(n)\}$$

equals 1.

Reference : *Downey, Jockusch, and Schupp, Asymptotic density and computably enumerable sets, Journal of Mathematical Logic, 13, No. 2 (2013)*

The γ-value of a set $A \subseteq \mathbb{N}$

A computable set R tries to approximate a complicated set A :

A : 100100100100 000101001001 010101111010 101010100111

R : 000010110111 010101000101 010001011010 101010100111

$\approx 1/2$ correct

$\approx 2/3$ correct

$\approx 3/4$ correct

$\approx 4/5$ correct

Take sup of the asymptotic correctness over all computable R's :

$$\gamma(A) = \sup_{R \text{ computable}} \underline{\rho}\{n \colon A(n) = R(n)\}$$

$$\text{where } \underline{\rho}(Z) = \liminf_n \frac{|Z \cap [0,n)|}{n}.$$

The γ-value of a set $A \subseteq \mathbb{N}$

A computable set R tries to approximate a complicated set A :

A : 100100100100 000101001001 010101111010 101010100111
R : 000010110111 010101000101 010001011010 101010100111

≈1/2 correct

≈2/3 correct

≈3/4 correct

≈4/5 correct

Take sup of the asymptotic correctness over all computable R's :

$$\gamma(A) = \sup_{R \text{ computable}} \underline{\rho}\{n\colon A(n) = R(n)\}$$

$$\text{where } \underline{\rho}(Z) = \liminf_n \frac{|Z \cap [0,n)|}{n}.$$

Some examples of values $\gamma(A)$

Recall

$$\gamma(A) = \sup_{R \text{ computable}} \underline{\rho}\{n\colon\ A(n) = R(n)\}$$

$$\text{where } \underline{\rho}(Z) = \liminf_n \frac{|Z \cap [0,n)|}{n}.$$

Theorem (Hirschfeldt, Jockusch, McNicholl, Schupp)

For any real $r \in [0,1]$, there is a set A with $\gamma(A) = r$. Moreover this value can either be both reached or not reached by some computable R in the definition of γ.

Γ-value of a Turing degree

Andrews, Cai, Diamondstone, Jockusch and Lempp (2013) looked at Turing degrees, rather than sets. They defined

$$\Gamma(A) = \inf\{\gamma(B) : \; B \text{ has the same Turing degree as } A\}$$

A smaller Γ value means that A is further away from computable.

Example

An oracle A is called computably dominated if every function that A computes is below a computable function. *They show :*

- If A is random and computably dominated, then $\Gamma(A) = 1/2$.
- If A is not computably dominated then $\Gamma(A) = 0$.

$\Gamma(A) > 1/2$ implies $\Gamma(A) = 1$

Fact (Hirschfeldt, Jockusch, McNicholl and Schupp)

If $\Gamma(A) > 1/2$ then A is computable (so that $\Gamma(A) = 1$).

The idea is to obtain B of the same Turing degree as A by "padding" :

- "Stretch" the value $A(n)$ over the whole interval $I_n = [(n-1)!, n!)$.
- Since $\gamma(B) > 1/2$ there is a computable R agreeing with B on more than half of the bits in almost every interval I_n.
- So for almost all n, the bit $A(n)$ equals the majority of values $R(k)$ where $k \in I_n$.

The Γ-question

Question (Γ-question, Andrews et al., 2013)

Is there a set $A \subseteq \mathbb{N}$ *such that* $0 < \Gamma(A) < 1/2$ *?*

•	? ? ? ? ? ? ? ? ? ?	•	× × × × × × ×	•
$\Gamma = 0$		$\Gamma = 1/2$		$\Gamma = 1$

Theorem

Let $A \in 2^{\mathbb{N}}$. *If* $\Gamma(A) < 1/2$ *then* $\Gamma(A) = 0$.

The proof uses the field of error-correcting codes.

Examples of $\Gamma(A) = 0$: infinitely often equal

We know that $A \subseteq \mathbb{N}$ not computably dominated implies $\Gamma(A) = 0$.

- We say $g : \mathbb{N} \to \mathbb{N}$ is infinitely often equal (i.o.e.) if $\exists^\infty n\ f(n) = g(n)$ for each computable function $f : \mathbb{N} \to \mathbb{N}$.
- We say that $A \subseteq \mathbb{N}$ is i.o.e. if A computes function g that is i.o.e.

Surprising fact : A is i.o.e $\Leftrightarrow$ A not computably dominated.

$\Rightarrow$ Suppose A computes a function g that equals infinitely often to every computable function. Then no computable function bounds g.

$\Leftarrow$ *Idea.* Suppose A computes a function g that is dominated by no computable function. Then g is infinitely often above the halting time of any computable total function.

New Examples of $\Gamma(A) = 0$: weaken infinitely often equal

We know A not computably dominated implies $\Gamma(A) = 0$.

Recall

We say that A is infinitely often equal (i.o.e.) if A computes a function g such that $\exists^\infty n \; f(n) = g(n)$ for each computable function $f : \mathbb{N} \to \mathbb{N}$.

We can weaken this :

Let $H \colon \mathbb{N} \to \mathbb{N}$ be computable. We say that A is *H-infinitely often equal* if A computes a function g such that $\exists^\infty n \; f(n) = g(n)$ for each computable function f *bounded by H*.

This appears to get harder for A the faster H grows.

A i.o.e. implies $\Gamma(A) = 0$

Let $H\colon \mathbb{N} \to \mathbb{N}$ be computable. We say that $A \subseteq \mathbb{N}$ is H-infinitely often equal if A computes a function g such that $\exists^\infty n \; f(n) = g(n)$ for each computable function f bounded by H.

Theorem (Monin, Nies)

Let A be $2^{(\alpha^n)}$-i.o.e. for some $\alpha > 1$. Then $\Gamma(A) = 0$.

New example of $\Gamma(A) = 0$

Recall : A is H-infinitely often equal if A computes a function g such that $\exists^\infty n\ f(n) = g(n)$ for each computable function f bounded by H.

Theorem

Let A be $2^{(\alpha^n)}$-i.o.e. for some computable $\alpha > 1$. Then $\Gamma(A) = 0$.

Proof sketch. First step : Let f be $2^{(\alpha^n)}$-i.o.e. Then for any $k \in \mathbb{N}$, f computes a function g that is $2^{(k^n)}$-i.o.e.

f(0) f(1) f(2) f(3) f(4) f(5) ... i.o.e. every comp. funct. $\leqslant 2^{(\alpha^n)}$

$\rightarrow$ $f(0)f(2)f(4)\ldots$ i.o.e. every comp. funct. $\leqslant n \mapsto 2^{(\alpha^{2n})}$

or $f(1)f(3)f(5)\ldots$ i.o.e. every comp. funct. $\leqslant n \mapsto 2^{(\alpha^{2n+1})}$

Iterating this $\rightarrow$ $f \geqslant_T g$ which i.o.e. every comp. funct. $\leqslant 2^{(k^n)}$

Proof sketch. Second step : g is $2^{(k^n)}$-i.o.e. implies $g \geqslant_T Z$ with $\Gamma(Z) \leqslant 1/k$.

$$\begin{array}{rcccc}
 & g(0) & g(1) & \dots & g(n) & \dots \\
 & = & = & \dots & = & \dots \\
Z: & \underbrace{\sigma_0}_{|\sigma_0|=k^0} & \underbrace{\sigma_1}_{|\sigma_1|=k^1} & \dots & \underbrace{\sigma_n}_{|\sigma_n|=k^n} & \dots
\end{array}$$

$$\begin{array}{rcccc}
\text{Computable } R: & \tau_0 & \tau_1 & \dots & \tau_n & \dots \\
 & & & \downarrow \text{(bit flip)} & & \\
\overline{R}: & \overline{\tau_0} & \overline{\tau_1} & \dots & \overline{\tau_n} & \dots \\
 & = & = & = & = & \\
 & j(0) & j(1) & \dots & j(n) & \dots
\end{array}$$

j equals g infinitely often. Then for infinitely many n, $\tau_n(i) \neq \sigma_n(i)$ everywhere. We have

$$|\tau_n| \geqslant (k-1) \sum_{i<n} |\tau_i|$$

Then the lim inf of fraction of places where R agrees with Z is bounded by $1/k$.

Proof sketch. Second step : g is $2^{(k^n)}$-i.o.e. implies $g \geqslant_T Z$ with $\Gamma(Z) \leqslant 1/k$.

$$
\begin{array}{rccccc}
 & g(0) & g(1) & \dots & g(n) & \dots \\
 & = & = & \dots & = & \dots \\
Z: & \underbrace{\sigma_0}_{|\sigma_0|=k^0} & \underbrace{\sigma_1}_{|\sigma_1|=k^1} & \dots & \underbrace{\sigma_n}_{|\sigma_n|=k^n} & \dots \\
 & & & & & \\
\text{Computable } R: & \tau_0 & \tau_1 & \dots & \tau_n & \dots \\
 & & & \downarrow \text{(bit flip)} & & \\
\overline{R}: & \overline{\tau_0} & \overline{\tau_1} & \dots & \overline{\tau_n} & \dots \\
 & = & = & = & = & \\
 & j(0) & j(1) & \dots & j(n) & \dots
\end{array}
$$

j equals g infinitely often. Then for infinitely many n, $\tau_n(i) \neq \sigma_n(i)$ everywhere. We have

$$|\tau_n| \geqslant (k-1)\sum_{i<n} |\tau_i|$$

Then the lim inf of fraction of places where R agrees with Z is bounded by $1/k$.

Proof sketch. Second step : g is $2^{(k^n)}$-i.o.e. implies $g \geqslant_T Z$ with $\Gamma(Z) \leqslant 1/k$.

$$
\begin{array}{rccccc}
 & g(0) & g(1) & \dots & g(n) & \dots \\
 & = & = & \dots & = & \dots \\
Z: & \underbrace{\sigma_0}_{|\sigma_0|=k^0} & \underbrace{\sigma_1}_{|\sigma_1|=k^1} & \dots & \underbrace{\sigma_n}_{|\sigma_n|=k^n} & \dots \\
 & & & & & \\
\text{Computable } R: & \tau_0 & \tau_1 & \dots & \tau_n & \dots \\
 & & & \downarrow \text{(bit flip)} & & \\
\overline{R}: & \overline{\tau_0} & \overline{\tau_1} & \dots & \overline{\tau_n} & \dots \\
 & = & = & = & = & \\
 & j(0) & j(1) & \dots & j(n) & \dots
\end{array}
$$

j equals g infinitely often. Then for infinitely many n, $\tau_n(i) \neq \sigma_n(i)$ everywhere. We have

$$|\tau_n| \geqslant (k-1) \sum_{i<n} |\tau_i|$$

Then the lim inf of fraction of places where R agrees with Z is bounded by $1/k$.

Nothing between 0 and 1/2

Theorem

Suppose $\Gamma(X) < 1/2 - \varepsilon$.

Then there is $k \in \mathbb{N}$ *and an* X*-computable sequence* $\{\tau_n\}_{n\in\mathbb{N}}$ *with* $|\tau_n| = 2^{n/k}$*, such that :*

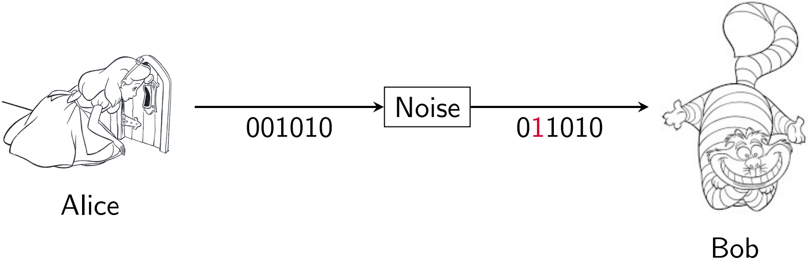
For every computable sequence $\{\sigma_n\}_{n\in\mathbb{N}}$ *with* $|\sigma_n| = |\tau_n|$*, there are infinitely many* n *such that* σ_n *agrees with* τ_n *on a fraction of at least* $1/2 + \varepsilon$ *bits.*

$\{\tau_n\}_{n\in\omega}$	τ_0	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	$\dots$
$\{\sigma_n\}_{n\in\omega}$	$\underbrace{\sigma_0}_{\geqslant 1/2+\varepsilon}$	σ_1	σ_2	$\underbrace{\sigma_3}_{\geqslant 1/2+\varepsilon}$	σ_4	σ_5	σ_6	σ_7	σ_8	$\dots$
$\{\sigma'_n\}_{n\in\omega}$	σ'_0	$\underbrace{\sigma'_1}_{\geqslant 1/2+\varepsilon}$	σ'_2	σ'_3	σ'_4	σ'_5	$\underbrace{\sigma'_6}_{\geqslant 1/2+\varepsilon}$	σ'_7	σ'_8	$\dots$

$\dots$

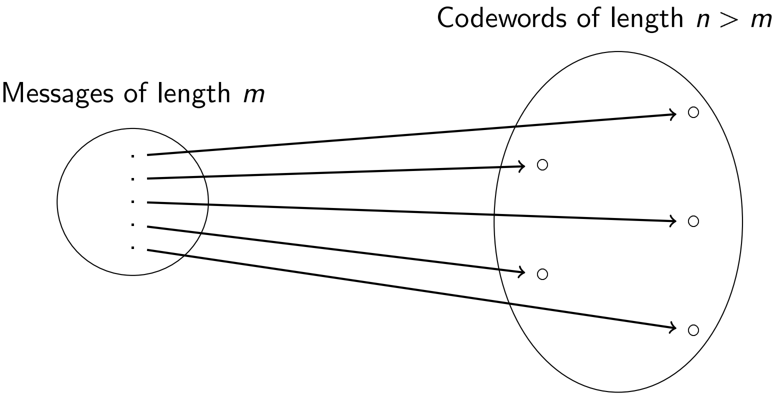
The error-correcting codes

We want to transmit a message of length m on a noisy chanel.



The error-correcting codes

We want to transmit a message of length m on a noisy chanel. We use an injection $\Phi : 2^m \to 2^n$ for $n > m$ in such a way that the strings in the range of Φ are pairwise as far as possible.



If δ is the smallest relative Hamming distance between two strings in the range of Φ, we can correct up to a fraction of $\delta/2$ errors.

Nothing between 0 and 1/4

Theorem (Basic error-correcting)

For any $\epsilon > 0$, there exists $\beta > 0$ sufficientky small such that for any n we have $2^{\beta n}$ many strings of length n with pairwise Hamming distance bigger than $1/2 - \varepsilon$.

Implication : We can correct up to a ratio of 1/4 of error by increasing the length a messages by a multiplicative factor.

Suppose now $\Gamma(X) < 1/4$. Let $\{\tau_n\}_{n\in\mathbb{N}}$ with $|\tau_n| = 2^{n/k}$, such that :

$\{\tau_n\}_{n\in\omega}$	τ_0	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	...
$\{\sigma_n\}_{n\in\omega}$	$\underbrace{\sigma_0}_{\geqslant 3/4+\varepsilon}$	σ_1	σ_2	$\underbrace{\sigma_3}_{\geqslant 3/4+\varepsilon}$	σ_4	σ_5	σ_6	σ_7	σ_8	...
$\{\sigma'_n\}_{n\in\omega}$	σ'_0	$\underbrace{\sigma'_1}_{\geqslant 3/4+\varepsilon}$	σ'_2	σ'_3	σ'_4	σ'_5	$\underbrace{\sigma'_6}_{\geqslant 3/4+\varepsilon}$	σ'_7	σ'_8	...
...										

Nothing between 0 and 1/4

$\{\tau_n\}_{n\in\omega}$	τ_0	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	$\dots$
$\{\sigma_n\}_{n\in\omega}$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	$\dots$
	$\geqslant 3/4+\varepsilon$			$\geqslant 3/4+\varepsilon$						
$\{\sigma'_n\}_{n\in\omega}$	σ'_0	σ'_1	σ'_2	σ'_3	σ'_4	σ'_5	σ'_6	σ'_7	σ'_8	$\dots$
		$\geqslant 3/4+\varepsilon$					$\geqslant 3/4+\varepsilon$			
$\dots$										

For any n we compute a sequence C_n of $2^{(\beta 2^{n/k})}$ many strings of length $2^{n/k}$ which all have pairwise Hamming distance larger than $1/4 - \varepsilon$.

From $\{\tau_n\}_{n\in\mathbb{N}}$, we compute the sequence $\{\rho_n\}_{n\in\mathbb{N}}$ of the strings of length $\beta 2^{n/k}$ whose code in C_n agrees with τ_n on more than $3/4 + \varepsilon$ bits.

Claim : *For every computable function g bounded by $2^{(\beta 2^{n/k})}$, there are infinitely many n such that $g(n) = \rho_n$ (seen as a binary string).*

Nothing between 0 and 1/2

We need to correct up to 1/2 errors. For this we need to use the list decoding theorem :

Theorem (List decoding theorem)

Let $\varepsilon > 0$*. For* $L \in \mathbb{N}$ *sufficiently large and* $\beta > 0$ *sufficiently small, there exists for any* $n \in \mathbb{N}$ *a set* C *of* $2^{\beta n}$ *many strings of length* n *such that :*
For any string σ *of length* n*, there are at most* L *elements* τ *of* C *such that* σ *agrees with* τ *on a fraction of bits of at least* $1/2 + \varepsilon$*.*