Some semigroup characterizations of the P-versus-NP problem

Jean-Camille Birget

To John Rhodes on his 81st birthday.
Goal:
Study the complexity classes \( P \) and \( NP \)
via functions, and semigroups of functions.
(More structured than just sets, or sets of languages.)

Here, “function” means \textbf{partial function}.

\textbf{Def.} \( f: A^* \rightarrow A^* \) is \textbf{polynomial-time computable} \iff there is a deterministic polynomial-time Turing machine that on input \( x \in \text{Dom}(f) \) outputs \( f(x) \).
(Hence \( \text{Dom}(f) \) is in \( P \).)

\textbf{Def.} \( f: A^* \rightarrow A^* \) is \textbf{polynomially balanced} \iff there exists a polynomial \( q \) such that for all \( x \in \text{Dom}(f) \):
\[ |f(x)| \leq q(|x|) \quad \text{and} \quad |x| \leq q(|f(x)|). \]

\textbf{Def.} (the semigroup of polyn.-time functions):
\( \text{fP} \) is the set of partial functions \( f: \{0, 1\}^* \rightarrow \{0, 1\}^* \) that are \textit{polynomially balanced}, and \textit{polynomial-time computable}.

\( \text{fP} \) is a monoid.

For \( P, NP \), and \( \text{fP} \), we will only use the alphabet \( \{0, 1\} \)
(for convenience).
Def. (One-way function in worst-case complexity).
A partial function $f: A^* \rightarrow A^*$ is one-way iff

- $f \in fP$, but
- there exists no deterministic polynomial-time algorithm which, for every input $y \in \text{Im}(f)$, outputs some $x \in f^{-1}(y)$.

Concept of inverse:
For $f: A^* \rightarrow A^*$, an inverse is $f': A^* \rightarrow A^*$ such that

$$f \circ f' \circ f = f.$$ 

Equivalently,

$$f(f'(y)) = y \quad \text{for all } y \in \text{Im}(f).$$

Equivalently,

$$f'(y) \in f^{-1}(y) \quad \text{for all } y \in \text{Im}(f).$$

Connection with NP:

Prop. (folklore).

One-way functions (in worst-case complexity) exist iff $P \neq NP$

Coroll.

The monoid $fP$ is regular iff $P = NP$.  

3
Prop. (place of $P$ and $NP$ in $fP$).

(1) $\forall f \in fP: \; \text{Im}(f) \in NP$.
(2) $\forall f \in fP: \; \text{if } f \text{ is regular then } \text{Im}(f) \in P$.
(3) For all $L \in NP$ there exists $f_L \in fP$ such that $L = \text{Im}(f_L)$.
    If $L \in P$, $f_L$ is regular.

Def. of $f_L$:
    Let $M_L$ be a nondet. (or det.) polyn.-time TM accepting $L$;
    $f_L(x, c) = x$ iff $c$ is an accepting computation of $M_L$ on input $x$
    ($f_L(x, c)$ is undefined otherwise).

In other words:
- $\text{Im}: f \mapsto \text{Im}(f)$ maps $fP$ onto $NP$;
- $\text{Im}$ maps the set of regular elements of $fP$ onto $P$.

Moreover:
- $NP$ is a retract of $fP$, by
  $L \in NP \iff f_L \in fP$ (depends on choice of $M_L$),
  $\text{Im}(f) \in NP \iff f \in fP$.
- This retract maps the regular elements of $fP$ onto $P$
  (if a det. TM is picked for $f_L$ when $L \in P$).

Prop.
The regular elements of $fP$ form a submonoid iff $P = NP$.

(The regular elements generate $fP$. So, the regular elements form a submonoid iff $fP = \text{the regular elements}$.)
Monoids of right-ideal morphisms

Def.: A right ideal of $A^*$ is $R \subseteq A^*$ such that $R \cdot A^* = R$. Equivalently, a right ideal is of the form $R = X A^*$, for any $X \subseteq A^*$. (Then “$X$ generates $R$ as a right ideal”.)

Def.: A prefix code in $A^*$ is $P \subseteq A^*$ such that no word in $P$ is a prefix of another word in $P$.

Fact.
• For any right ideal $R$ there exists a unique prefix code $P_R$ such that $R = P_R \cdot A^*$.
• If $R$ is a right ideal, and $R \in P$, then $P_R \in P$.
• If $X \in P$, then $XA^* \in P$.

Def.:
A right ideal morphism of $A^*$ is $h: A^* \to A^*$ such that $\forall x \in \text{Dom}(h), \forall w \in A^*: h(xw) = h(x) \cdot w$.

Fact. $\text{Dom}(h)$ and $\text{Im}(h)$ are right ideals.

Notation.
• $\text{domC}(h)$, called the domain code, is the prefix code that generates $\text{Dom}(h)$ as a right ideal.
• $\text{imC}(h)$, called the image code, is the prefix code that generates $\text{Im}(h)$ as a right ideal.

Fact. $\text{imC}(f) \subseteq f(\text{domC}(f))$ (possibly $\neq$).
Def. (monoid of polyn.-time right-ideal morphisms):
\[ \mathcal{RM}^P = \{ f \in fP : f \text{ is a right ideal morphism of } \{0,1\}^* \} \]
\[ \mathcal{RM}^P \text{ is a submonoid of } fP. \]

Lemma. If an element \( f \in \mathcal{RM}^P \) has an inverse in \( fP \) then \( f \) also has an inverse in \( \mathcal{RM}^P \).

Coroll. \( \mathcal{RM}^P \) is regular iff \( P = NP \).

Prop.
- \( \mathcal{RM}^P \) is \( J^0 \)-simple (i.e., the only ideals are \( \{0\} \) and \( \mathcal{RM}^P \)).
- \( fP \) is not \( J^0 \)-simple.
- \( fP \) and \( \mathcal{RM}^P \) are not isomorphic.

Prop. \( \mathcal{RM}^P \) has trivial group of units (\( fP \) does not).
Encoding over the prefix code \{00, 01, 11\}:

\[
\text{code}(0) = 00, \quad \text{code}(1) = 01
\]

For \( x \in \{0, 1\}^* \),

\[
\text{code}(x) = \text{concatenation of the codes of the letters in } x.
\]

**Def. of code}(f) for \( f \in \mathfrak{f}P \):**

For \( x \in \text{Dom}(f) \), \( v \in \{0, 1\}^* \),

\[
\text{code}(f): \quad \text{code}(x) 11 v \mapsto \text{code}(f(x)) 11 v.
\]

Properties:

\[
\text{code}(f) \in \mathcal{RM}^P,
\]
\[
\text{Dom(code}(f)) = \text{code(Dom}(f)) 11 \{0, 1\}^*,
\]
\[
\text{Im(code}(f)) = \text{code(Im}(f)) 11 \{0, 1\}^*.
\]

**Fact.**

- \( \text{code}: \mathfrak{f}P \to \mathcal{RM}^P \) is an injective semigroup homomorphism.
- \( f \in \mathfrak{f}P \) is regular iff \( \text{code}(f) \in \mathcal{RM}^P \) is regular.

**Relation between \( \mathfrak{f}P \) and \( \mathcal{RM}^P \):**

\[
\mathfrak{f}P \overset{\text{code}}{\leftrightarrow} \mathcal{RM}^P \overset{\subset}{\subseteq} [\text{id}]_J^{0} \overset{\subset}{\subseteq} \mathfrak{f}P
\]

where \( [\text{id}]_J^{0} = \text{Rees quotient of the } J\text{-class of id in } \mathfrak{f}P \).
**Evaluation maps**

In general, an *evaluation map* is

\[
\text{eval}(\text{prog}, x) = f_{\text{prog}}(x), \quad \text{or} \\
\text{ev}(\text{prog}, x) = (\text{prog}, f_{\text{prog}}(x)).
\]

Evaluation maps for \( fP \) do not belong to \( fP \) (since \text{eval} would not have polyn.-bounded complexity nor balance).

**Evaluation maps for a fixed polynomial \( q(.) \):**

Consider programs \( w \) for det. I/O TMs, with built-in time and balance bounds \( \leq q(.) \).
Such a program \( w \) computes \( \phi_w \in fP \).
For such a program \( w \) and \( x \in \text{Dom}(\phi_w) \), define

\[
\text{ev}_q(\text{code}(w) 11 u) = \text{code}(w) 11 \phi_w(x).
\]

Then \( \text{ev}_q \in fP \).

**Fact.** Let \( q(n) = a \cdot (n^2 + 1) \), with \( a > 2 \). Then

\( \text{ev}_q \) is regular in \( fP \) \iff \( fP \) is regular \( \quad (\iff P = NP) \).
Finite generation of $fP$:
For any $fP$-program $w$ (polyn.-bounded, but not necessarily by $q(.)$), i.e., for any $\phi_w \in fP$:

$$
\phi_w(x) = \pi'_{2|w'|+2} \circ \text{contr} \circ \text{recontr}^{2m} \circ \text{ev}_q \\
\circ \text{reexpand}^{2m} \circ \text{expand} \circ \pi_{\text{code}(w)\text{11}}(x).
$$

Here,

$$
m = \log_2(\sum \text{coefficients} + \text{degree of } q(.)).
$$

$$
\pi_{\text{code}(w)\text{11}}(x) = \text{code}(w)\text{11 }x.
$$

\text{reexpand}^{2m} \circ \text{expand} creates an exponential amount of padding, so \text{ev}_q can be applied.

\text{contr} \circ \text{recontr}^{2m} removes the padding.

$$
\pi'_{2|w'|+2} \text{ removes (a modified) } \text{code}(w)\text{11}.
$$

Prop.
The monoid $fP$ is finitely generated.

Moreover, $fP$ is finitely generated by regular elements.

Prop.
The word problem of $fP$ is co-r.e., but not r.e.; hence $fP$ is not finitely presented.
Theorem. \( \mathcal{RM}^p \) is not finitely generated.

(\( \mathcal{RM}^p \) has an \( \text{ev}_q \) function, but padding is not possible.)

Def. For any polynomial \( q(.) \), let \( \mathcal{RM}^q \) denote the submonoid of \( \mathcal{RM}^p \) generated by functions with complexity and balance \( \leq q(.) \).

Theorem. \( \mathcal{RM}^q \) is not finitely generated.

But \( \mathcal{RM}^q \) is contained in a 4-generated submonoid of \( \mathcal{RM}^p \).

Coroll.
(Strict complexity hierarchy of submonoids in \( \mathcal{RM}^p \)).

There is a sequence of polynomials \( (q_i(.) : i \in \mathbb{N}) \),
\[
q_i(x) = a_i x^{k_i} + a_i, \quad k_i < k_{i+1} \text{ in } \mathbb{N}, \quad 1 < a_i < a_{i+1},
\]
such that
\[
\mathcal{RM}^{q_i} \subsetneq \mathcal{RM}^{q_{i+1}} \quad \text{for all } i,
\]
\[
\bigcup_{i \in \mathbb{N}} \mathcal{RM}^{q_i} = \mathcal{RM}^p.
\]

This is an unusual complexity hierarchy:
Each \( \mathcal{RM}^{q_i} \) contains functions of arbitrarily high polynomial complexity and balance.
Congruences on $\mathcal{RM}^P$ – Definitions

**End-equivalence** $\equiv_{\text{end}}$:
For prefix codes $P_1, P_1 \subset \{0, 1\}^*$ in $\mathcal{P}$,

$P_1 \equiv_{\text{end}} P_2$ iff $P_1\{0, 1\}^*$ and $P_2\{0, 1\}^*$ intersect the same right ideals.

For $f_1, f_2 \in \mathcal{RM}^P$,

$f_1 \equiv_{\text{end}} f_2$ iff $\text{domC}(f_1) \equiv_{\text{end}} \text{domC}(f_2)$ and $f_1, f_2$ agree on $\text{Dom}(f_1) \cap \text{Dom}(f_2)$.

**Bounded end-equivalence** $\equiv_{\text{bd}}$:
For prefix codes $P_1, P_1 \subset \{0, 1\}^*$ in $\mathcal{P}$,

$P_1 \equiv_{\text{bd}} P_2$ iff $P_1 \equiv_{\text{end}} P_2$ and there exists a total $\beta : \mathbb{N} \to \mathbb{N}$ such that for all $x_1 \in P_1, x_2 \in P_2$:

$x_1 \parallel_{\text{pref}} x_2$ implies $|x_1| \leq \beta(|x_2|)$ and $|x_2| \leq \beta(|x_1|)$.

For $f_1, f_2 \in \mathcal{RM}^P$,

$f_1 \equiv_{\text{bd}} f_2$ iff $\text{domC}(f_1) \equiv_{\text{bd}} \text{domC}(f_2)$ and $f_1, f_2$ agree on $\text{Dom}(f_1) \cap \text{Dom}(f_2)$.

**Prop.**:

$P_1 \equiv_{\text{bd}} P_2$ iff $P_1\{0, 1\}^\omega = P_2\{0, 1\}^\omega$.

**Prop.**:

$f_1 \equiv_{\text{bd}} f_2$ iff $f_1$ and $f_2$ determine the same function on $\{0, 1\}^\omega$.  

11
Polynomial end-equivalence  $\equiv_{\text{poly}}$:

For prefix codes $P_1, P_1 \subset \{0, 1\}^*$ in $P$, 
\[ P_1 \equiv_{\text{poly}} P_2 \quad \text{iff} \]
\[ \bullet \ P_1 \equiv_{\text{end}} P_2 \quad \text{and} \]
\[ \bullet \ \text{there exists a polynomial } p(.) \text{ such that for all } x_1 \in P_1, \ x_2 \in P_2: \]
\[ x_1 \parallel_{\text{pref}} x_2 \ \text{implies} \ |x_1| \leq p(|x_2|) \quad \text{and} \quad |x_2| \leq p(|x_1|). \]

For $f_1, f_2 \in \mathcal{RM}^P$,
\[ f_1 \equiv_{\text{poly}} f_2 \quad \text{iff} \]
\[ \bullet \ \text{domC}(f_1) \equiv_{\text{poly}} \text{domC}(f_2), \quad \text{and} \]
\[ \bullet \ f_1, f_2 \ \text{agree on} \ \text{Dom}(f_1) \cap \text{Dom}(f_2). \]

Similarly, $\equiv_{E3}$ is defined like $\equiv_{\text{poly}}$, using composites of exponentials (instead of polynomials).

Prop.  $\equiv_{\text{end}}, \ \equiv_{\text{bd}}, \ \equiv_{E3}, \ \equiv_{\text{poly}},$ are congruences on $\mathcal{RM}^P$.

Let $\mathcal{M}_{\text{end}}^P, \mathcal{M}_{\text{bd}}^P, \mathcal{M}_E^P, \mathcal{M}_{\text{poly}}^P$ be the respective quotient monoids:
\[ \text{i.e., } \mathcal{M}_{\text{poly}}^P = \mathcal{RM}^P/\equiv_{\text{poly}}, \text{ etc.} \]
Relation between $\mathcal{RM}^P$ and its quotients:

$$
\begin{array}{c}
\mathcal{RM}^P \\
1:1 \\
\mathcal{RM}^{n+o(n)} \rightarrow M_{\text{poly}}^P \rightarrow M_{E3}^P \rightarrow M_{bd}^P \rightarrow M_{\text{end}}^P \\
\end{array}
$$

where $\mathcal{RM}^{n+o(n)}$ is the submonoid of $\mathcal{RM}^P$ of functions with complexity and balance $\leq n + o(n)$.

The triangle of maps is a commutative diagram.

Properties:

- $\mathcal{RM}^{n+o(n)}$ is non-regular. But it maps onto $M_{\text{poly}}^P$.
- $M_{\text{poly}}^P$ is regular iff $\mathcal{RM}^P$ is regular, iff $P = \text{NP}$.
  $M_{\text{poly}}^P$ is finitely generated; hence $M_{E3}^P$ etc. are finitely generated.
- $M_{E3}^P$, $M_{bd}^P$, and $M_{\text{end}}^P$ are regular.
- $M_{bd}^P$ has exactly two non-zero $D$-classes.
  $M_{bd}^P$ acts faithfully on $\{0, 1\}^\omega$; in fact,
  $M_{bd}^P$ is the monoid of the action of $\mathcal{RM}^P$ on $\{0, 1\}^\omega$.
- $M_{\text{end}}^P$ is congruence-simple, so it is the end of the chain;
  i.e., $\equiv_{\text{end}}$ is is the coarsest non-trivial congruence on $\mathcal{RM}^P$.
  $M_{\text{end}}^P$ has only one non-zero $D$-class.
- The group of units of $M_{\text{poly}}^P$, $M_{E3}^P$, and $M_{bd}^P$, is the
  Richard Thompson group $V$ (a.k.a. $G_{2,1}$).
Conclusion

It is interesting to represent $P$ and $NP$ by semigroups. These semigroups are defined in a simple and natural way, have interesting properties, and are obviously connected to the $P$-versus-$NP$ problem. So these semigroups are worth studying.

But it is not clear whether these semigroups will be useful for settling the $P$-versus-$NP$ problem.