COMPLEXITY CLASS OPERATORS

ROBERT SANDERS

A *complexity class operator* op is an inclusion-preserving automorphism on the set of all complexity classes, written as $\mathsf{op} \cdot \mathsf{C}$ for a complexity class C. Thus, if $\mathsf{C} \subseteq \mathsf{D}$, then $\mathsf{op} \cdot \mathsf{C} \subseteq \mathsf{op} \cdot \mathsf{D}$. Complexity Zoology's knowledge of operators consists of inequalities of the form $\mathsf{op}_1 \leq \mathsf{op}_2$, meaning that $(\mathsf{op}_1 \cdot \mathsf{C})^A \subseteq (\mathsf{op}_2 \cdot \mathsf{C})^A$ for each class C and oracle A, and quadratic relations of the form $\mathsf{op}_1 \cdot \mathsf{op}_2 = \mathsf{op}_3 \cdot \mathsf{op}_4$, meaning that $(\mathsf{op}_1 \cdot \mathsf{op}_2 \cdot \mathsf{C})^A = (\mathsf{op}_3 \cdot \mathsf{op}_4 \cdot \mathsf{C})^A$ for each class C and oracle A.

1. Definitions

The definitions of the following complexity class operators preserve relativization. In other words, if an operator op is defined by the property that

$$\mathsf{op} \cdot \mathsf{C} = \{\mathscr{L} \subseteq \Sigma^* : \varphi(\mathscr{L}, \mathsf{C})\}$$

for any complexity class C, then the relativized version of $\mathsf{op} \cdot \mathsf{C}$ is

$$(\mathsf{op} \cdot \mathsf{C})^A = \{\mathscr{L} \subseteq \Sigma^* : \varphi(\mathscr{L}, \mathsf{C}^A)\}.$$

The simplest operators are id, the identity operator; co, which swaps "yes" and "no" answers to each decision problem; and cocap, which takes the intersection of a class with its complement.

Definition. For each complexity class C, we set

$$\begin{aligned} \mathsf{id} \cdot \mathsf{C} &:= \{\mathscr{L} \subseteq \Sigma^* : \mathscr{L} \in \mathsf{C}\} = \mathsf{C}, \\ \mathsf{co} \cdot \mathsf{C} &:= \{\mathscr{L} \subseteq \Sigma^* : \Sigma^* \setminus \mathscr{L} \in \mathsf{C}\}, \\ \mathsf{cocap} \cdot \mathsf{C} &:= \{\mathscr{L} \subseteq \Sigma^* : \mathscr{L} \in \mathsf{C} \,\&\, \mathscr{L} \in \mathsf{co} \cdot \mathsf{C}\} = \mathsf{C} \cap (\mathsf{co} \cdot \mathsf{C}). \end{aligned}$$

A class is **symmetric** if $\mathsf{C} = \mathsf{co} \cdot \mathsf{C}$ with respect to every oracle.

For example, the class P is symmetric, while NP is not, because there is an oracle A relative to which $\mathsf{NP}^A \neq \mathsf{coNP}^A$ (although, of course, this is an open problem in the absence of an oracle.

The poly operator adds a polynomial-length advice string to each input. To be precise, we denote by $|\mathscr{O}(n^*)|$ the set of all functions $p : \mathbb{N} \to \Sigma^*$ such that $|p(n)| = \mathscr{O}(n^k)$ for some $k \in \mathbb{N}$. A function $p \in |\mathscr{O}(n^*)|$ is regarded as an *advice function* when $p(n)$ is given as an argument for each input of length n.

Definition. For a complexity class C, we define

$$\mathsf{poly} \cdot \mathsf{C} = \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}, p \in |\mathscr{O}(n^*)|)(\forall x \in \Sigma^*)[x \in \mathscr{L} \iff \langle x, p(|x|)\rangle \in \mathscr{L}']\}.$$

We allow advice functions to map to the null string ε of length zero. In the case of tuples, $\langle x, \varepsilon\rangle$ should be understood to be x, so that, as we will see, $\mathsf{poly} \cdot \mathsf{C}$ always contains C. For most classes with polynomial advice, we write $\mathsf{poly} \cdot \mathsf{C} = \mathsf{C}/\mathsf{poly}$; we have, for instance, P/poly, $\mathsf{NP}/\mathsf{poly}$, and $\mathsf{BQP}/\mathsf{poly}$.

The operators $\oplus$, N, and P are all defined in terms of certificates, strings whose lengths are polynomials of the length of the original input. Let $\mathscr{O}(n^*)$ denote the set of all functions $p : \mathbb{N} \to \mathbb{N}$ such that $p(n) = \mathscr{O}(n^k)$ for some $k \in \mathbb{N}$; then, for a quantifier Q, we can define an operator op_Q by

$$\mathsf{op}_Q \cdot \mathsf{C} := \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}, p \in \mathscr{O}(n^*))(\forall x \in \Sigma^*)[x \in \mathscr{L} \iff (Qy \in \Sigma^{p(|x|)})[\langle x, y\rangle \in \mathscr{L}']]\}.$$

The aforementioned operators are then equal to op_Q for different choices of Q.

Definition. The operators $\oplus$, N, and P are defined as follows for a complexity class C:
- $\oplus \cdot \mathsf{C} := \mathsf{op}_Q \cdot \mathsf{C}$, where $(Qy \in S)$ means "for an odd number of $y \in S$."
- $\mathsf{N} \cdot \mathsf{C} := \mathsf{op}_Q \cdot \mathsf{C}$, where $(Qy \in S)$ means $(\exists y \in S)$.
- $\mathsf{P} \cdot \mathsf{C} := \mathsf{op}_Q \cdot \mathsf{C}$, where $(Qy \in S)$ means "for more than 1/2 of all $y \in S$."

$\oplus$ is read as "parity."

The bounded probabilistic operator BP is defined similarly.

Definition. For each complexity class C,

$$\begin{aligned}\mathsf{BP} \cdot \mathsf{C} := \{\mathscr{L} \subseteq \Sigma^* :& (\exists \mathscr{L}', p \in \mathscr{O}(n^*))(\forall x \in \Sigma^*)[[x \in \mathscr{L} \implies (\exists_{>2/3}\, y \in \Sigma^{p(|x|)})[\langle x, y\rangle \in \mathscr{L}']] \\ & \& \,[x \notin \mathscr{L} \implies (\exists_{>2/3}\, y \in \Sigma^{p(|x|)})[\langle x, y\rangle \notin \mathscr{L}']]]\},\end{aligned}$$

where $(\exists_{>2/3}\, y \in \Sigma^{p(|x|)})$ is understood to mean "for more than 2/3 of all $y \in \Sigma^{p(|x|)}$."

All of these operators are named in such a way that they suggest the definitions of common complexity classes; for example, $\mathsf{NP} = \mathsf{N} \cdot \mathsf{P}$, $\mathsf{PP} = \mathsf{P} \cdot \mathsf{P}$, $\mathsf{BPP} = \mathsf{BP} \cdot \mathsf{P}$, and $\oplus\mathsf{P} = \oplus \cdot \mathsf{P}$.

Finally, we have the operator $\mathsf{C} \mapsto \mathsf{P}^{\mathsf{C}}$, which maps to C to P with C-oracle, as well as exppad, which adds an exponential length of zeros to input, generally for the purpose of buying additional computational time.

Definition. For every complexity class C,

$$\mathsf{P}^{\mathsf{C}} := \{\mathscr{L} \subseteq \Sigma^* : (\exists A \in C)[\mathscr{L} \in \mathsf{P}^A]\} = \bigcup_{A \in C} \mathsf{P}^A,$$

where the languages in C have been identified with their decision functions.

The above operator is used in the definition of the polynomial hierarchy: for every $n \in \mathbb{N}$, $\Delta^{\mathsf{P}}_{n+1} = \mathsf{P}^{\Sigma^{\mathsf{P}}_n}$.

Definition. Let $\mathscr{O}(2^{\text{poly}})$ denote the set of all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(n) = \mathscr{O}(2^{p(n)})$ for some polynomial function $p : \mathbb{N} \to \mathbb{N}$. Then, for a complexity class C,

$$\mathsf{exppad} \cdot \mathsf{C} := \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}, f \in \mathscr{O}(2^{\text{poly}}))[x \in \mathscr{L} \iff x0^{f(|x|)} \in \mathscr{L}']\}.$$

NEXP, for example, is not defined to be $\mathsf{N} \cdot \mathsf{EXP}$, but rather $\mathsf{exppad} \cdot \mathsf{NP}$.

2. Properties of Complexity Classes

Proving the properties of complexity operators often requires that the underlying complexity classes themselves have certain regularity properties. First, every complexity class of interest should be *nontrivial* in the sense that it contains a nonempty language not equal to Σ^*. We also expect that if $\mathscr{L} \in \mathsf{C}$, then any languages that are reducible to $\mathscr{L}$ in polynomial-time are also in C.

Definition. A complexity class C is **polynomial-time self-reducible** if for every $\mathscr{L} \in \mathsf{C}$ and every function $f \in \mathsf{FP}$,

$$f^{-1}[\mathscr{L}] = \{x \in \Sigma^* : f(x) \in \mathscr{L}\} \in \mathsf{C}.$$

Every class in this project is relativizingly nontrivial and polynomial-time self-reducible, so that for each oracle A, if $f \in \mathsf{FP}^A$ and $\mathscr{L} \in \mathsf{C}^A$ then $f^{-1}[\mathscr{L}] \in \mathsf{C}^A$. As a result, P lies at the bottom of Complexity Zoology's inclusion hierarchy.

Proposition. *If C is a nontrivial, polynomial-time self-reducible complexity class, then $\mathsf{P} \subseteq \mathsf{C}$.*

Proof. Fix a nontrivial language $\mathscr{L} \in \mathsf{C}$, so that $\mathscr{L} \neq \emptyset$ and $\mathscr{L} \in \Sigma^*$. Then there exists $x_1 \in \mathscr{L}$ and $x_0 \notin \mathscr{L}$.

Now suppose $\mathscr{L}' \in \mathsf{P}$.. Then define $f : \Sigma^* \to \Sigma^*$ to be

$$f(x) = \begin{cases} x_1 & \text{if } x \in \mathscr{L}', \\ x_0 & \text{if } x \notin \mathscr{L}'. \end{cases}$$

We have $f \in \mathsf{FP}$, since it can be determined whether or not $x \in \mathscr{L}'$ in polynomial-time, and then writing x_1 or x_0 can be accomplished in constant time. Therefore $\mathscr{L}' = f^{-1}[\mathscr{L}] \in \mathsf{C}$ by polynomial-time self-reducibility, so we can conclude that $\mathsf{P} \subseteq \mathsf{C}$. $\square$

Additionally, complexity classes should be closed under joins and projections. The *join* of a pair of languages $\mathscr{L}, \mathscr{L}' \subseteq \Sigma^*$ is

$$\mathscr{L} \oplus \mathscr{L}' = \{x \in \Sigma^* : (x = 0y \,\&\, y \in \mathscr{L}) \text{ or } (x = 1y \,\&\, y \in \mathscr{L}')\}.$$

The *0-projection* of a language $\mathscr{L}$ is

$$\{x \in \Sigma^* : 0x \in \mathscr{L}\},$$

and the *1-projection* is defined similarly.

3. Relations and Inclusions

Proposition. *The* id, co, *and* cocap *operators satisfy the following properties:*

(1) $\mathsf{cocap} \leq \mathsf{co}$ *and* $\mathsf{cocap} \leq \mathsf{id}$*;*
(2) co *is involutive, so that* $\mathsf{co} \cdot \mathsf{co} = \mathsf{id}$*;*
(3) $\mathsf{co} \cdot \mathsf{cocap} = \mathsf{cocap} \cdot \mathsf{co} = \mathsf{cocap}$.

Proof. (1) and (2) are immediate from the definitions of the operators. For (3), we have

$$\begin{aligned} \mathsf{cocap} \cdot \mathsf{co} \cdot \mathsf{C} &= (\mathsf{co} \cdot \mathsf{C}) \cap (\mathsf{co} \cdot \mathsf{co} \cdot \mathsf{C}) \\ &= (\mathsf{co} \cdot \mathsf{C}) \cap \mathsf{C} \\ &= \mathsf{cocap} \cdot \mathsf{C}, \end{aligned}$$

and

$$\begin{aligned} \mathscr{L} \in \mathsf{co} \cdot \mathsf{cocap} \cdot \mathsf{C} &\iff \Sigma^* \setminus \mathscr{L} \in \mathsf{cocap} \cdot \mathsf{C} \\ &\iff \Sigma^* \setminus \mathscr{L} \in \mathsf{C} \,\&\, \Sigma^* \setminus \mathscr{L} \in \mathsf{co} \cdot \mathsf{C} \\ &\iff \mathscr{L} \in \mathsf{co} \cdot \mathsf{C} \,\&\, \mathscr{L} \in \mathsf{co} \cdot \mathsf{co} \cdot \mathsf{C} \\ &\iff \mathscr{L} \in \mathsf{co} \cdot \mathsf{C} \,\&\, \mathscr{L} \in \mathsf{C} \\ &\iff \mathscr{L} \in \mathsf{cocap} \cdot \mathsf{C}. \end{aligned}$$

$\square$

For many operators, it is the case that $\mathsf{C} \in \mathsf{op} \cdot \mathsf{C}$ for every C, because the definitions of these classes include an additional certificate or advice string.

Proposition. $\mathsf{id} \subseteq \mathsf{op}$, *where* $\mathsf{op} = \mathsf{poly}, \oplus, \mathsf{BP}, \mathsf{P}, \mathsf{N}$ *or* exppad.

Proof. Fix $\mathscr{L} \in \mathsf{C}$. Then $\mathscr{L} \in \mathsf{op} \cdot \mathsf{C}$ for each possible choice of op:

- If $\mathsf{op} = \mathsf{poly}$, take $\mathscr{L}' = \mathscr{L}$ and $p(n) = \varepsilon$ for all $n \in \mathbb{N}$ in the definition of $\mathsf{poly} \cdot \mathsf{C}$.
- If $\mathsf{op} = \oplus, \mathsf{BP}, \mathsf{P},$ or N, take $\mathscr{L}' = \mathscr{L}$ and $p(n) = 0$ for all $n \in \mathbb{N}$ in the definition of $\mathsf{op} \cdot \mathsf{C}$.
- If $\mathsf{op} = \mathsf{exppad}$, take $\mathscr{L}' = \mathscr{L}$ and $f(n) = \varepsilon$ for all $n \in \mathbb{N}$ in the definition of $\mathsf{exppad} \cdot \mathsf{C}$.

□

Since the condition $\mathscr{L} \in \mathsf{BP} \cdot \mathsf{C}$ is a strengthening of the condition that $\mathscr{L} \in \mathsf{P} \cdot \mathsf{C}$, the following is immediate.

Proposition. $\mathsf{BP} \leq \mathsf{P}$.

We next consider some commutativity properties.

Proposition. $\mathsf{co} \cdot \mathsf{op} = \mathsf{op} \cdot \mathsf{co}$, *where* $\mathsf{op} = \mathsf{BP}, \mathsf{P},$ *or* poly.

Proof. For each of the possible choices of op, the definition of $\mathsf{op} \cdot \mathsf{C}$ has the following form:

$$op \cdot \mathsf{C} := \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}) \psi(\mathscr{L}, \mathscr{L}')\},$$

where $\psi(\mathscr{L}, \mathscr{L}')$ is a proposition having the property that

$$\psi(\mathscr{L}, \Sigma^* \setminus \mathscr{L}') \Longleftrightarrow \psi(\Sigma^* \setminus \mathscr{L}, \mathscr{L}').$$

Thus,

$$\begin{aligned}
\mathsf{co} \cdot \mathsf{op} \cdot \mathsf{C} &= \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}) \psi(\Sigma^* \setminus \mathscr{L}, \mathscr{L}')\} \\
&= \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{C}) \psi(\mathscr{L}, \Sigma^* \setminus \mathscr{L}')\} \\
&= \{\mathscr{L} \subseteq \Sigma^* : (\exists \mathscr{L}' \in \mathsf{co} \cdot \mathsf{C}) \psi(\mathscr{L}, \mathscr{L}')\} \\
&= \mathsf{op} \cdot \mathsf{co} \cdot \mathsf{C}
\end{aligned}$$

for each possible choice of op. □

A similar argument, based on the structure of te definitions of the relevant operators, can be used to show that poly commutes with $\oplus$, N, and P.

Proposition. *If complexity classes are assumed to be polynomial-time self-reducible, then* $\mathsf{poly} \cdot \mathsf{op} = \mathsf{op} \cdot \mathsf{poly}$*, where* $\mathsf{op} = \oplus, \mathsf{N},$ *or* poly.

Proof. We say that $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{op} \cdot \mathsf{C}$ if there exist $\mathscr{L}' \in \mathsf{C}$, $p \in \mathscr{O}(n*)$, and $q \in |\mathscr{O}(n^*)|$ such that for every $x \in \Sigma^*$,

$$x \in \mathscr{L} \Longleftrightarrow (Qy \in \Sigma^{p(|\langle x, q(|x|) \rangle|)})[\langle \langle x, q(|x|) \rangle, y \rangle \in \mathscr{L}'],$$

where Q is the quantifier in the definition of the operator that is being considered. Similarly, we say that $\mathscr{L} \in \mathsf{op} \cdot \mathsf{poly} \cdot \mathsf{C}$ if there exist $\mathscr{L}' \in \mathsf{C}$, $p \in \mathscr{O}(n*)$, and $q \in |\mathscr{O}(n^*)|$ such that for every $x \in \Sigma^*$,

$$x \in \mathscr{L} \Longleftrightarrow (Qy \in \Sigma^{p(|x|)})[\langle \langle x, y \rangle, q(|\langle x, y \rangle|) \rangle \in \mathscr{L}'].$$

The condition $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{op} \cdot \mathsf{C}$ is equivalent to the condition that there are $\mathscr{L}' \in \mathsf{C}$, $\bar{p} \in \mathscr{O}(n^*)$, and $q \in |\mathscr{O}(n^*)|$ such that for all $x \in \Sigma^*$,

$$x \in \mathscr{L} \Longleftrightarrow (Qy \in \Sigma^{\bar{p}(|x|)})[\langle \langle x, q(|x|) \rangle, y \rangle \in \mathscr{L}'].$$

For instance, if $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{op} \cdot \mathsf{C}$, then we can set $\bar{p}(n) = p(N)$, where $N = |\langle x, q(|x|)\rangle|$ for $|x| = n$. Likewise, in the conditions for $\mathscr{L} \in \mathsf{op} \cdot \mathsf{poly} \cdot \mathsf{C}$ we can replace q with a $\bar{q}$ so that

$$x \in \mathscr{L} \iff (Qy \in \Sigma^{p(|x|)})[\langle\langle x, y\rangle, \bar{q}(|x|)\rangle \in \mathscr{L}'].$$

The rewritten conditions for $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{op} \cdot \mathsf{C}$ and $\mathscr{L} \in \mathsf{op} \cdot \mathsf{poly} \cdot \mathsf{C}$ are then equivalent to each other because a mapping between $\langle\langle x, z\rangle, y\rangle$ and $\langle\langle x, y\rangle, z\rangle$ is polynomial-time computable. $\square$

Proposition. *If complexity classes are assumed to be polynomial-time self-reducible, then* $\mathsf{co} \cdot \oplus = \oplus \cdot \mathsf{co}$.

Finally, we consider the properties of the operator $\mathsf{C} \mapsto \mathsf{P}^{\mathsf{C}}$.

Proposition. *For any complexity class* C*,*

(1) $\mathsf{C} \subseteq \mathsf{P}^{\mathsf{C}}$*;*
(2) $\mathsf{co} \cdot \mathsf{C} \subseteq \mathsf{P}^{\mathsf{C}}$*;*
(3) $\mathsf{co} \cdot \mathsf{P}^{\mathsf{C}} = \mathsf{P}^{\mathsf{co} \cdot \mathsf{C}} = \mathsf{P}^{\mathsf{C}}$.

Proof. If $\mathscr{L} \in \mathsf{C}$ and A is the decision function for $\mathscr{L}$, then $\mathscr{L} \subseteq \mathsf{P}^A \subseteq \mathsf{P}^{\mathsf{C}}$. Hence $\mathsf{C} \subseteq \mathsf{P}^{\mathsf{C}}$. Moreover, P^A is a symmetric class for every A, and so

$$\begin{aligned}
\mathscr{L} \in \mathsf{co} \cdot \mathsf{P}^{C} &\iff \Sigma^* \setminus \mathscr{L} \in \mathsf{P}^{\mathsf{C}} \\
&\iff (\exists A \in \mathsf{C})[\Sigma^* \setminus \mathscr{L} \in \mathsf{P}^A] \\
&\iff (\exists A \in \mathsf{C})[\mathscr{L} \in \mathsf{P}^A] \\
&\iff \mathscr{L} \in \mathsf{P}^{\mathsf{C}},
\end{aligned}$$

and

$$\begin{aligned}
\mathscr{L} \in \mathsf{P}^{\mathsf{co} \cdot \mathsf{C}} &\iff (\exists A \in \mathsf{C})[\mathscr{L} \in \mathsf{P}^{1-A}] \\
&\iff (\exists A \in \mathsf{C})[\mathscr{L} \in \mathsf{P}^A] \\
&\iff \mathscr{L} \in \mathsf{P}^{\mathsf{C}},
\end{aligned}$$

because $\mathsf{P}^A = \mathsf{P}^{1-A}$ for every oracle A. Thus, (1) and (3) are true. (2) then follows immediately, because $\mathsf{C} \subseteq \mathsf{P}^{\mathsf{C}} \implies \mathsf{co} \cdot \mathsf{C} \subseteq \mathsf{co} \cdot \mathsf{P}^{\mathsf{C}} \implies \mathsf{co} \cdot \mathsf{C} \subseteq \mathsf{P}^{\mathsf{C}}$. $\square$

Proposition. *For any complexity class non-trivial, polynomial-time self reducible class* C *that is closed under joins,* $\mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}} = \mathsf{P}^{\mathsf{poly} \cdot \mathsf{C}}$ *and* $\mathsf{BP} \cdot \mathsf{P}^{\mathsf{C}} = \mathsf{P}^{\mathsf{BP} \cdot \mathsf{C}}$.

Proof of first equation. First, we show that it is unconditionally the case that $\mathsf{P}^{\mathsf{poly} \cdot \mathsf{C}} \subseteq \mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}}$. Suppose that $\mathscr{L} \in \mathsf{P}^{\mathsf{poly} \cdot \mathsf{C}}$. Then there is a polynomial-time algorithm with A-oracle that computes $\mathscr{L}$, where A is a decision function for a language $\mathscr{L}' \in \mathsf{poly} \cdot \mathsf{C}$. By the definition of the poly operator, there exists a language $\mathscr{L}'' \in \mathsf{C}$ and an advice function $p \in |\mathscr{O}(n^*)|$ such that $x \in \mathscr{L}'$ if and only if $\langle x, p(|x|)\rangle \in \mathscr{L}''$.

Let A' indicate the decision function for $\mathscr{L}''$. Also, let $f \in \mathscr{O}(n^*)$ denote time bound for the P^A algorithm for $\mathscr{L}$, so that the question of whether $x \in \mathscr{L}$ is decided in at most $f(|x|)$ computational steps. Define $P : \mathbb{N} \to \Sigma^*$ so that, for each $n \in \mathbb{N}$, $P(n)$ is the concatenation $p(0)p(1)\dots p(f(n))$.

The following algorithm in $\mathsf{poly} \cdot \mathsf{P}^{A'}$ decides whether $x \in \mathscr{L}$:

(1) The advice function is P. Note that $P \in |\mathscr{O}(n^*)|$, because for sufficiently large n $|P(n)|$ is at most $f(n)|p(f(n))|$.
(2) Follow the P^A algorithm for $\mathscr{L}$ exactly, except when there is an oracle call.

(3) When an oracle call to A occurs with the string $y \in \Sigma^*$, replace it with an oracle call to A' with the string $\langle y, p(|y|)\rangle$. This oracle call is possible because $P(|x|)$ contains the advice strings for all y that are short enough for the P^A algorithm to be able to query the oracle.

Thus, we have $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{P}^{A'} \subseteq \mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}}$, and we can conclude that $\mathsf{P}^{\mathsf{poly}\cdot\mathsf{C}} \subseteq \mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}}$ in all cases.

For the inclusion $\mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}} \subseteq \mathsf{P}^{\mathsf{poly}\cdot\mathsf{C}}$, suppose that $\mathscr{L} \in \mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}}$. This means that there exists a P^A algorithm that decides $\mathscr{L}$ when provided with some advice function $p \in |\mathscr{O}(n^*)|$, where A is the decision function of some $\mathscr{L}'\Sigma^* \to \Sigma$ according to the following rules:

- If $x = 0\,\langle y, z\rangle$, then $A'(x)$ is equal to the zth bit of $p(|y|)$.
- If $x = 1y$, then $A'(x) = A(y)$.

The language $\mathscr{L}''$ determined by A' is the join of two languages. One, which we will call $\mathscr{L}_0''$, is the set of all $\langle y, z\rangle$ such that the zth bit of $p(|y|)$ is 1; the second language is $\mathscr{L}'$.

We claim that $\mathscr{L}''$ lies in $\mathsf{poly} \cdot \mathsf{C}$. To prove this, it is enough to show that $\mathscr{L}_1'' \in \mathsf{P}/\mathsf{poly}$. Then $\mathsf{P}/\mathsf{poly} \subseteq \mathsf{poly} \cdot \mathsf{C}$ (we know that $\mathsf{P} \subseteq \mathsf{C}$ because C si assumed to be nontrivial and polynomial-time self-reducible), and $\mathscr{L}' \in \mathsf{poly} \cdot \mathsf{C}$ by assumption, so $\mathscr{L}'' \in \mathsf{poly} \cdot \mathsf{C}$ by the hypothesis that C, and therefore $\mathsf{poly} \cdot \mathsf{C}$, is closed under joints.

To see that $\mathscr{L}_1'' \in \mathsf{P}/\mathsf{poly}$, let $P \in |\mathscr{O}(n^*)|$ be the function defined by the concatenation $P(n) = p(0)p(1)\dots p(n)$. Then, given $\langle y, z\rangle$, P can be used as an advie function to check whether the zth bit of $p(|y|)$ is 1.

Hence $\mathscr{L}'' \in \mathsf{polyC}$. To show that $\mathscr{L} \in \mathsf{P}^{\mathsf{poly}\cdot\mathsf{C}}$, we show that $\mathscr{L} \in P^{A'}$. The following is a $\mathsf{P}^{A'}$ algorithm for deciding whether $x \in \mathscr{L}$:

(1) First, extract the advice string $p(|x|)$ from the A'-oracle. Make the oracle queries $0\,\langle x, j\rangle$, $j \leq |p(|x|)|$ until the entirety of $p(|x|)$ has been recorded.
(2) Carry out the rest of the computation according to the $\mathsf{poly} \cdot \mathsf{P}^A$ algorithm. Replace oracle queries to A about the string y with oracle queries to A' about the string y.

Therefore $\mathscr{L} \in \mathsf{P}^{\mathsf{poly}\cdot\mathsf{C}}$, concluding the proof that $\mathsf{P}^{\mathsf{poly}\cdot\mathsf{C}} = \mathsf{poly} \cdot \mathsf{P}^{\mathsf{C}}$. □

The first of these equations is true because advice can be moved between the polynomial-time computation and the oracle class, while the latter equation is true because randomness in computation is equivalent to randomness in the oracle. The class C must satisfy the regularity properties discussed in the previous section.