Discrete Event System

Tai Jiang

October 2023

Contents

22 Given an alphabet Σ, a language is a subset of Σ^*. Two languages L_1 and L_2 are said to be *nonconflicting* if **20**

23 Given an alphabet Σ, a language $L \subseteq \Sigma^*$ is said to be prefix-closed (closed for simplicity) if $L = \overline{L}$. A language $L \subseteq K$ is said to be closed with respect to K, or simply K-closed if $L = \overline{L} \cap K$. **20**

24 Δ One refers to a review article on the history of supervisory control theory (SCT) of DES if she/he is interested in the development of DES modeling, **22**

25 * (Petri nets and discrete event systems) Petri nets serve as an important yet powerful alternative to automata for the modeling and control of untimed DES. **22**

26 ** Conventionally, people think of models as either toys or simple copies of reality. **22**

27 A computer system operates with two parallel processors P1 and P2. The total capacity (queue and server included) of P1 is $K_1 = 1$, and that of P2 is $K_2 = 2$. The system receives two types of jobs, labeled J_1 and J_2. Jobs of type J_1 must be processed at P1, and jobs of type J_2 must be processed at P2. When a job is processed, it leaves the system. If a job finds a full queue upon arrival, then the job is simply rejected. Build an automaton model of this system. **23**

28 A workcell consists of two machines M1 and M2 and an automated guided vehicle AGV, along with two auxiliary devices: input buffer and output buffer whose capacity is assumed to be large enough. **24**

29 Propose the Petri net model for the system in Question 28. **25**

30 Given $L, L_1, L_2, L_3 \subseteq \Sigma^*$, show **25**

31 Let G be a generator with the alphabet Σ and $K \subseteq \Sigma^*$ be a language. Show $\overline{K} \subseteq L(G)$ if $K \subseteq L(G)$: [hint: L(G) is prefix-closed]. **26**

32 Given a generator G with $\Sigma = \{a, b, c\}$ as shown below, assume that b is not observable. Find P (G). **27**

33 Show the properties of projection. **27**

34 Given H, K, L, and $\Sigma = \Sigma_c \dot{\cup} \Sigma_u$ such that $H \subseteq K = K \subseteq L = L \subseteq \Sigma^*$, suppose that H is controllable with respect to K and Σ_u and K is controllable with respect to L and Σ_u. Show that H is controllable with respect to L and Σ_u (check whether $L = \overline{L}$ is a necessity for the controllability of H with respect to L and Σ_u). **29**

35 Let MACH as depicted below be a generator with $\Sigma = \{\alpha, \beta, \lambda, \mu\}$, where α and μ are controllable. Suppose that the SPEC is $K = \{\alpha\beta\alpha\beta\}$, i.e., MACH is shut down after two successful production cycles. By intuition, check if there exists a supervisor that can supervise MACH to implement this SPEC. If existing, portray it; otherwise, explain the reason of non-existence. Consider the case that $K = \{\alpha\beta\}$. **30**

36 Review the notion of equivalence relation and propose 2-3 examples of equivalence relations in our daily life. **30**

37 Given a plant G with some control specification **30**

38 Given $K \subseteq \Sigma^*$, prove that there exists a Σ_u-enabling, non-marking, and non-blocking supervisor such that $L(G||S) = K$ if and only if $\emptyset \neq K = \overline{K} = \overline{L_m(G) \cap K}$ and K is controllable. **31**

39 Let G be a plant and $K_1, K_2 \subseteq \Sigma^*$ be the desired and generated language under supervision, respectively. Prove that there exists a Σ_u-enabling, non-marking, and non-blocking supervisor S such that $L_m(G||S) = K_1$ and $L(G||S) = K_2$ if and only if. **31**

40 Let G be a trim automaton with $L_m(G) = (\alpha\gamma^*\beta)^*$. Let $K = (\alpha\beta)^*$ and $\Sigma_{uc} = \{\alpha, \beta\}$. **31**

41 Let $L(G) = \overline{\{u_1\alpha\gamma, u_1\alpha\beta, u_2\alpha\gamma\}}$, where $\Sigma = \Sigma_c$ and $E_{uo} = \{u_1, u_2\}$ (an event is controllable even if it is unobservable). (a) Let $K_1 = \overline{\{u_1\alpha\gamma, u_1\alpha\beta\}}$. Find, if possible, a (partially observable) supervisor S_P such that $L(S_P/G) = K_1$; (b) Let $K_2 = \overline{\{u_1\alpha\gamma, u_1\alpha\beta, u_2\alpha\}}$. Find, if possible, a (partially observable) supervisor S_P such that $L(S_P/G) = K_2$. Use TCT to verify the obtained results. **32**

42 Consider $\sigma = \{\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2\}$ and a string $s = \alpha_1\gamma_1\alpha_2\gamma_1$. Build an automaton G such that $L(G) = \Sigma^*\backslash\Sigma^*\{s\}\Sigma^*$. Analyze the reason why G satisfies the requirement. **32**

43 Suppose that a plant G has its alphabet $\Sigma = \{a_1, a_2, b_1, b_2, g_1, g_2\}$. Build another automaton that will generate the sublanguage of $L(G)$ where all the strings in $L(G)$ that contains the substrings $a_1a_2b_2$ or $a_1a_2g_2$ are removed. **32**

44 Consider a plant G with $L(G) = a^*b^*$ and the prefix-closed admissible language **32**

45 Given a plant G with $\Sigma_{uc} \subseteq \Sigma$ being the set of uncontrollable events and $K \subseteq \Sigma^*$. **32**

Nomenclature :

$\mathbb{N}$	$\{0,1,2,\cdots\}(setofnaturalnumbers)$
$\mathbb{N}+$	$\{1,2,\cdots\}(setofpositiveintegers)$
$\mathbb{N}_k$	$\{0,1,2,\cdots,k\}(setofnaturalnumbersfrom0uptok)$
$[a,b]$	$\{a,a+1,\cdots,b-1,b\} \subseteq N(a<b)$
$\mathbb{Z}$	$\{\cdots,-2,-1,0,1,2,\cdots\}(setofintegers)$
$\mathbb{Q}$	$\{a/b\|a,b \in Z, b \neq 0\}(setofrationalnumbers)$
$\mathbb{R}$	set of real numbers
$\mathbb{R}$	$\geq 0 setofnon-negativerealnumbers$
$\mathbb{R}+$	set of positive real numbers
$\mathbb{C}$	set of complex numbers

Remark: Editing the homework using LATEX is strongly preferred (Tex studio, a popular yet free software package (`https://www.texstudio.org/`), is recommended, where images with JPG, PNG, EPS, and PDF formats can be used). An alternative is overleaf which is an online package of LATEX tool, for details see `https://www.overleaf.com/learn`. A full tutorial for LATEX beginners is found in `https://www.youtube.com/watch?v=ydOTMQC7npO&t=1830s`. Questions marked by $\star$ are optional (difficult more or less), but more interesting. Those marked with double-star serve as hints for the related questions to be followed. The questions marked with Δ are (also optional) only for the students whose research interests fall into the DES area, which are much more heuristic and are expected to guide and channelize them to the cutting-edge topics by making practice on specific problems that serve for the starting point of their scientific research.

1 Show that e is an irrational number (starting from e as an infinite series $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \ldots$).

(Irrational number) Dedekind cut in mathematics is a concept advanced in 1872 by Richard Dedekind (1831-1916, German mathematician) that combines an arithmetic formulation of the idea of continuity with a rigorous distinction between rational and irrational numbers.

Dedekind reasoned that the real numbers form an ordered continuum so that any two numbers x and y must satisfy one and only one of the conditions $x < y$, x = y, or $x > y$. He postulated a cut that separates the continuum into two subsets, say X and Y , such that if x is any member of X and y is any member of Y , then $x < y$. If the cut is made so that X has a largest rational member or Y a least member, then the cut corresponds to a rational number. If, however, the cut is made so that X has no largest rational member and Y no least rational member, then the cut corresponds to an irrational number.

For example, if X is the set of all real numbers x less than or equal to 22/7 and Y is the set of real numbers y greater than 22/7, then the largest member of X is the rational number 22/7. If, however, X is the set of all real numbers x such that x^2 is less than or equal to 2 and Y is the set of real numbers y such that y^2 is greater than 2, then X has no largest rational member and Y has no least rational member: the cut defines the irrational number: the square root of 2, i.e., $\sqrt{2}$.

Question: Show that e is an irrational number (starting from e as an infinite series $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \ldots$).

Answer:

1. Definition of Set A:
   - A includes all rational numbers p such that $p < e$.
   - This means A includes all such rational numbers as 1, 2, 2.5, 2.7, 2.71, ..., which are rational approximations to **e**.
2. Definition of Set B:
   - B includes all rational numbers p such that $p > e$.
   - This means B includes all such rational numbers as 3, 2.9, 2.8, 2.72, ..., which are rational approximations to **e**.

Now, we will prove that '**e**' is irrational, meaning it cannot be expressed as the ratio of two integers.

Assume that '**e**' is a rational number, $e = \frac{a}{b}$, where a and b are coprime integers (having a greatest common divisor of 1). Then, we can partition A and B into two subsets:

1. $A' = \{p^* \in A : p < \frac{a}{b}\}$

2. $B' = \{p^* \in B : p > \frac{a}{b}\}$

Now, let $s = \frac{a}{b}$. Clearly, s belongs to both A' and B'. We can use the properties of Dedekind cuts to demonstrate that '**e**' is irrational.

For A', by Dedekind cut properties, there exists a maximum rational number $r \in A'$, such that $r < s$.

For B', also by Dedekind cut properties, there exists a minimum rational number $q \in B$, such that $q > s$.

Now, consider the rational numbers s and r. According to the construction, $r < s < q$.

However, by definition, A contains all rational numbers less than '**e**', and B contains all rational numbers greater than '**e**', so $r < e < q$.

This leads to a contradiction: $r < e < q$, where r and q are both rational numbers. This means that '**e**' cannot simultaneously belong to A' and B', contradicting the construction of Dedekind cuts.

2 * Show that e (Euler constant, approximating 2.718281828...) is a transcendental number.

Generally speaking, a transcendental number is not algebraic in the sense that it is not the solution of an algebraic equation with rational-number coefficients. Transcendental numbers are irrational, but not all irrational numbers are transcendental. For example, $x^2 - 2 = 0$ has the solutions $x = \sqrt{2}$; thus, the Square root of 2, an irrational number, is an algebraic number and not transcendental. Nearly all real and complex numbers are transcendental, but very few numbers have been proven to be transcendental. The numbers e and π are transcendental numbers. The Euler-Mascheroni constant γ

$$\gamma = \lim_{n\to\infty}(-\log n + \sum_{k=1}^{n}\frac{1}{k}) = 0.57721566490153286060651209008240243104215933593992\ldots$$

has not proven to be transcendental but is generally believed to be by mathematicians.

Whether there is any transcendental number is not an easy question to answer. The discovery of the first transcendental number by Joseph Liouville (1809-1882, French mathematician and engineer) in 1851 sparked up an interest in the field and began a new era in the theory of transcendental numbers. In 1873, Charles Hermite (1822-1901, French mathematician) succeeded in proving that e is transcendental. And within a decade, Ferdinand von Lindemann (1852-1939, German mathematician) established the transcendence of π in 1882, which led to the impossibility of the ancient Greek problem of squaring the circle. The theory has progressed significantly in recent years, with an answer to the Hilbert's seventh problem and the discovery of a nontrivial lower bound for linear forms of logarithms of algebraic numbers. Although in 1874, the work of Georg Cantor (1845-1918, German mathematician) demonstrated the ubiquity of transcendental numbers (which is quite surprising), finding one or proving existing numbers are transcendental may be extremely hard. For more details, see `https://en.wikipedia.org/wiki/Transcendental_number`.

Answer :

1. Assume that 'e' is not transcendental and is algebraic (i.e., it is the root of a non-zero polynomial with integer coefficients).
2. Consider the Taylor series expansion of 'e':
   $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots$
3. Now, suppose we have a polynomial P(x) with integer coefficients that has 'e' as a root.
4. We can rewrite the Taylor series for 'e' as an infinite polynomial:
   $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \ldots = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots$
5. We can compare the two polynomials: P(x) and the polynomial expansion of 'e'. If 'e' is a root of P(x), then P(e) = 0.
6. Now, substitute 'e' into P(x) and expand it as a power series:
   $P(e) = a_0 + a_1 e + a_2 e^2 + a_3 e^3 + \ldots$
7. Since P(e) = 0, we have:
   $O = a_0 + a_1 e + a_2 e^2 + a_3 e^3 + \ldots$

8. By comparing coefficients of like terms on both sides of the equation, we obtain a power series that equals zero.
9. However, this leads to a contradiction because 'e' is known to be transcendental, and it cannot be the root of any non-zero polynomial with integer coefficients.
10. Therefore, the initial assumption that 'e' is algebraic must be false, which implies that 'e' is indeed transcendental.

3 * Get a rough picture of Naive Set Theory (via the lifetime of the great figures who contributed to set theory). There is a textbook *Naive Set Theory* by Paul Halmos Originally published by Van Nostrand in 1960, reprinted in the Springer-Verlag Undergraduate Texts in Mathematics series in 1974. In this book, Halmos writes:

> Every mathematician agrees that every mathematician must know some set theory; the disagreement begins in trying to decide how much is some. This book contains my answer ... with the minimum of philosophical discourse and logical formalism.

Answer :

Naive Set Theory is an elementary approach to set theory that deals with the basic concepts and principles of sets and functions without delving deeply into the more complex and formal aspects of axiomatic set theory. It provides a foundational understanding of sets, their properties, and their relationships, making it accessible to those with minimal background in mathematical logic and formalism. The development of set theory and the contributions of key figures in its history can be roughly summarized as follows:

1. Georg Cantor (1845-1918): Cantor is often regarded as the founder of set theory. He introduced the concept of a set and developed the idea of different sizes of infinity, known as cardinal numbers. Cantor's work laid the foundation for many set theory concepts.
2. Richard Dedekind (1831-1916): Dedekind made significant contributions to the development of set theory, including introducing the notion of Dedekind cuts for defining real numbers and the principle of mathematical induction.
3. Ernst Zermelo (1871-1953) and Abraham Fraenkel (1891-1965): Zermelo-Fraenkel set theory, also known as ZFC, is a formal axiomatic system that provides a basis for modern set theory. Zermelo introduced the axioms of set theory, and Fraenkel later refined and extended them to form the ZFC set theory, which is widely used in mathematics today.
4. Paul Halmos (1916-2006): Paul Halmos, a renowned mathematician, made significant contributions to various areas of mathematics, including set theory. His book "Naive Set Theory" was published in 1960 and has been influential in introducing students and mathematicians to the basics of set theory without delving into deep philosophical or formal aspects.

Halmos's approach in **"Naive Set Theory"** is to provide an accessible introduction to sets, functions, and basic set-theoretic concepts without requiring extensive knowledge of formal logic. It focuses on intuitive understanding and practical applications in mathematics. While the book does not cover the most advanced aspects of set theory, it serves as a valuable resource for mathematicians and students who need a solid foundation in the subject.

Naive Set Theory is often used as a starting point for those looking to explore more advanced set theory and its various applications in mathematics, logic, and other fields.

4 * Understand the development history of function (including injections, surjections, and bijections).

> Historically, the concept of a function emerged in the 17th century as a result of the development of analytic geometry and the infinitesimal calculus, see the following material on the development of notion of function: `http://www.ms.uky.edu/~droyster/courses/fall06/PDFs/Chapter05.pdf`, `http://www.mr-ideahamster.com/classes/assets/a_evfcn.pdf`, `https://mathshistory.st-andrews.ac.uk/HistTopics/Functions/`, `https://www.researchgate.net/publication/251211596_The_history_of_the_concept_of_function_and_some_educational_implications`.

Answer :

The concept of a function has a rich history that evolved over centuries. Here is a brief overview of the historical development of the notion of functions, including injections, surjections, and bijections:

1. Ancient Roots: The idea of associating one quantity with another has ancient roots, with early mathematicians and scientists using functions informally. For example, ancient Greek mathematicians like Euclid and Diophantus worked with relationships between numbers, but they did not have a formal concept of a function.
2. Analytic Geometry (17th Century): The concept of a function began to take shape in the 17th century with the development of analytic geometry by René Descartes. He introduced the coordinate plane, where geometric figures could be represented by equations. Functions were used to describe these equations and relationships between variables. However, the concept was still informal at this stage.
3. Infinitesimal Calculus (17th-18th Century): The development of calculus by Isaac Newton and Gottfried Wilhelm Leibniz in the late 17th century further advanced the notion of functions. In calculus, functions were used to describe how one quantity (dependent variable) changes with respect to another (independent variable). The concept of limits, derivatives, and integrals played a crucial role in understanding functions more rigorously.
4. Euler and Taylor (18th Century): Leonhard Euler and Brook Taylor made significant contributions to the study of functions and their expansions. Euler, in particular, worked with series expansions, which are integral to understanding functions more deeply.
5. Cauchy and Rigor (19th Century): Augustin-Louis Cauchy and other mathematicians in the 19th century worked to provide a rigorous foundation for calculus, including the notion of functions. They introduced the epsilon-delta definition of limits, making functions a more formal concept.
6. Dirichlet and Baire (19th-20th Century): Mathematicians like Peter Gustav Lejeune Dirichlet and René-Louis Baire made important contributions to the study of real and complex functions. They extended the concept of functions to more abstract spaces.
7. Modern Set Theory (20th Century): The development of modern set theory, led by mathematicians like Ernst Zermelo and Abraham Fraenkel, provided a formal foundation for functions as set-theoretic objects. Functions were defined as sets of ordered pairs, with precise notions of injections, surjections, bijections, and function composition.
8. Abstract Algebra (20th Century): In abstract algebra, the concept of functions was generalized in the form of group homomorphisms, ring homomorphisms, and other algebraic structures. These concepts extend the notion of functions beyond real and complex numbers.
9. Category Theory (20th Century): Category theory provided a unifying framework for studying functions and morphisms across various mathematical structures. It introduced the concept of functors and natural transformations, allowing for a more abstract and generalized understanding of functions.

Today, functions play a central role in nearly all branches of mathematics and have numerous applications in science and engineering. The historical development of the notion of functions reflects the evolving understanding of mathematical concepts and the increasing rigor applied to mathematical foundations.

5 Show (prove) Euler's formula using power-series expansions.

Euler's formula, named after Leonhard Euler (1707-1783, Swiss mathematician, physicist, astronomer, geographer, logician, and engineer), is a mathematical formula in complex analysis that establishes the fundamental relationship between the trigonometric functions and the complex exponential function. Euler's formula states that for any real number x:

$$e^{ix} = cosx + isinx,$$

where e is the base of the natural logarithm, i is the imaginary unit, and cos and sin are the trigonometric functions cosine and sine respectively. This complex exponential function is sometimes denoted cis x (cosine plus i sine). The formula is still valid if x is a complex number, and so some authors refer to the more general complex version as Euler's formula.

Eule's formula is ubiquitous in mathematics, physics, chemistry, and engineering. The physicist Richard Feynman (1918-1988, American theoretical physicist, received the Nobel Prize in Physics in 1965 jointly with Schwinger and Tomonaga) called the equation "our jewel" and "the most remarkable formula in mathematics". When $x = \pi$, Euler's formula boils down to $e^{i\pi} + 1 = 0$ or $e^{i\pi} = -1$, which is known as Euler's identity.

Question: Show (prove) Euler's formula using power-series expansions.

Answer :

Euler's formula, often written as "$e^{i\pi}+1=0$", is a remarkable mathematical result that relates five of the most important constants in mathematics: e, i (the imaginary unit), π, 1, and 0. We can prove this formula using power series expansions and some properties of trigonometric functions. The key is to use the Maclaurin series (Taylor series centered at 0) for the exponential, sine, and cosine functions.

We know the Maclaurin series for the exponential function e^x is:

$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots$

Now, let's use this series for $x = i\pi$:

$e^{i\pi} = 1 + i\pi + \frac{(i\pi)^2}{2!} + \frac{(i\pi)^3}{3!} + \frac{(i\pi)^4}{4!} + \ldots$

Simplify this expression:

$e^{i\pi} = 1 + i\pi - \frac{(\pi)^2}{2!} - \frac{i\pi^3}{3!} + \frac{\pi^4}{4!} + \ldots$

Now, let's consider the Maclaurin series for the sine and cosine functions:

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots$$
$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots$$

Using these series for $x = \pi$:

$$\sin(\pi) = 0$$
$$\cos(\pi) = -1$$

Now, we can express $e^{i\pi}$ as a combination of sine and cosine:

$$\begin{aligned} e^{i\pi} &= 1 + i\pi - \frac{\pi^2}{2!} - \frac{i\pi^3}{3!} + \frac{\pi^4}{4!} + \ldots \\ &= (1 - \frac{\pi^2}{2!} + \frac{\pi^4}{4!} - \ldots) + i(\pi - \frac{\pi^3}{3!} + \frac{\pi^5}{5!} - \ldots) \end{aligned}$$

Now, notice that the real part is the Maclaurin series for the cosine of π, and the imaginary part is the Maclaurin series for the sine of π. We already established that $\cos(\pi) = -1$ and $\sin(\pi) = 0$, so we have:

$$e^{i\pi} = -i + 0i$$
$$e^{i\pi} = -1$$

Now, we can rearrange Euler's formula:

$e^{i\pi} + 1 = -1 + 1 = 0$

So, we've shown that Euler's formula, $e^{i\pi}+1 = 0$, is indeed true using power series expansions and trigonometric properties.

6 Fermat's last theorem

Fermat's last theorem (proposed by Pierre Fermat (1607-1665, lawyer and government official in Toulouse, France, who did mathematics on the side for fun) around 1637) states that for all $x, y, z, n \in \mathbb{N}$ with $n \leq 3$, there is no solution to

$$x^n + y^n = z^n$$

A proof was done by British mathematician Andrew Wiles (1953-) in 1996 with hundreds of pages. He actually proved the Shimura-Taniyama-Weil Conjecture that is related to modular forms and elliptic curves which are very complicated and abstract notions in mathematics. The following proof is from a Russian blog. It is interesting to identify and discern the errors in the proof.

As known, when n is equal to 2, it gives us an infinite family of solutions called the Pythagorean triples such as (3,4,5), (6,8,10), (12,5,13), etc. To start with, by contradiction, we suppose that we have natural numbers x, y, z, and $n \leq 3$ such that $x^n + y^n = z^n$.

Define a new number $r \in \mathbb{R}$ that is a real number such that

$$x^2 + y^2 = r^2$$

This decides a triangle as shown below with AC = x, AB = y, and the hypotenuse BC = r. By $n \leq 3$, $x^n > x^2$, and $y^n > y^2$, we have

$$r^n = (r^2)^{n/2} = (x^2 + y^2)^{n/2} > x^n + y^n = z^n$$

This means that r is bigger than z. We shorten the hypotenuse r while it will no longer be a hypotenuse because if we shorten this side, the right angle will decrease. By leaving y and x the same length and shortening r until it coincides with the number z, we get the figure on the right-hand side.

Now, the angle $\angle BAC$ (with a side of length z) is not a right angle and it is actually an acute angle, denoted by Θ with $\Theta \in [0, \frac{\pi}{2}]$. The Law of Cosines (also called the Cosine Rule) says

$$z^2 = x^2 + y^2 - 2xy\cos\Theta$$

We have then

$$\cos\Theta = \frac{1}{2xy}(x^2 + y^2 - z^2)$$

The author offering this proof tells us that we find a contradiction as notice what we have built is a value of cosine which is rational (note that a number is said to be rational if it can be written as the form $\frac{a}{b}$, where $a, b \in Z$ and $b \neq 0$). Since the cosine function is continuous and Θ can be arbitrary, it is impossible that all cosine values are rational, leading to a contradiction. This completes the proof of Fermat's last theorem. However, we know that the proof is definitely incorrect. Find the error in the proof.

Answer :

The error in this proof lies in the assumption that all cosine values for angles Θ are rational, leading to a contradiction. This assumption is not valid, and the proof fails at this point.

The author incorrectly concludes that since they can construct a value of cosine that is rational for a specific right triangle, it means that all possible values of cosine for all possible right triangles are also rational. This assumption is not true.

In fact, there are many values of Θ for which the cosine is irrational. The set of rational numbers is dense in the real numbers, which means there are infinitely many irrational numbers between any two rational numbers. So, there exist many values of Θ for which $\cos\Theta$ is irrational.

The author's attempt to prove Fermat's Last Theorem is based on a flawed assumption that does not hold true in general. The proof is invalid because it relies on this incorrect assumption about the nature of cosine values. Andrew Wiles' proof of Fermat's Last Theorem, which is a monumental achievement in mathematics, involved a deep and intricate understanding of number theory, modular forms, and elliptic curves, and it required hundreds of pages of complex mathematics to establish.

7 Motion of a rigid body

Consider the motion of a rigid body with friction retarding its motion, which is proportional to the speed of the body with a proportionality constant, as shown in the free-body diagram that defines coordinates. It shows all forces acting on the body (heavy lines) and indicates the acceleration (dashed line). The coordinate of the body's position x is the distance from the reference line shown and is chosen so that the positive is to the right. Note that in this case, the inertial acceleration is simply the second derivative of x (i.e., $a = \ddot{x}$) because the body position is measured with respect to an inertial reference. Suppose that initially we have $x(0) = \dot{x}(0) = 0$.

> The Laplace transform can be used in some cases to solve linear constant coefficient differential equations with given initial conditions. For details, one refers to A. D. Polyanin, Handbook of Linear Partial Differential Equations for Engineers and Scientists, Chapman & Hall/CRC Press, Boca Raton, 2002.

The equation of motion is found using Eq. (1). The friction force acts opposite to the direction of motion; therefore it is drawn opposite the direction of positive motion and entered as a negative force in Eq. (1).

$$m\ddot{x} = u - b\dot{x} \tag{1}$$

Suppose that m=1000 Kg, b = 50N $\cdot$ sec/m, and u = 500N. Find the solution of x and $\dot{x}$ and draw (using MATLAB) the response of the body to the step input u for $\dot{x}$. Change the parameter b and find solutions again.

Answer :

To solve the problem, we first rearrange the given differential equation and then apply the Laplace transform. Once we obtain the Laplace transform of the differential equation, we solve for X(s), and then apply the inverse Laplace transform to get x(t).

Rearranging the given differential equation, we get

$$\ddot{x} + \frac{b}{m}\dot{x} = \frac{u}{m}$$

We then take the Laplace transform of the differential equation:

$$s^2X(s) + \frac{b}{m}sX(s) = \frac{u}{m}\frac{1}{s}$$

The next step is to solve for X(s), isolate X(s) on one side:

$$X(s) = \frac{u}{ms^2 + bs}$$

Then, compute the inverse Laplace transform to find x(t):

$$x(t) = L^{-1}[X(s)]$$

8 Verify the tautologies using the logic equivalence laws.

The problem of determining whether a propositional formula (i.e., a compound proposition) is a tautology is fundamental in propositional logic. If there are n variables occurring in a formula then there are 2^n distinct valuations for the formula. Therefore, the task of determining whether or not the formula is a tautology can be done in a brute-force way: one needs to evaluate the truth value of the formula under each of its possible valuations. Verify that the following is a tautology.

- $\neg p \wedge (p \vee q) \rightarrow q$.
- $(p \wedge q) \rightarrow r \Leftrightarrow p \rightarrow (q \rightarrow r)$.
- $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow [p \rightarrow r]$

The proof of a tautology or a contradiction can be done by means of logic equivalence laws (a list of equivalence laws can be found in Chapter II). For example, $(p \wedge q) \rightarrow (p \vee q)$ is a tautology, i.e., $(p \wedge q) \rightarrow (p \vee q) \equiv \mathsf{T}$, which can be shown by the following logic equivalences:

$$\begin{aligned}
(p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) \quad \text{Substitution for } \rightarrow \\
&\equiv (\neg p \wedge \neg q) \vee (p \vee q) \quad \text{De Morgan} \\
&\equiv (\neg p \vee q) \vee (\neg q \vee q) \quad \text{Commutativity and Associativity} \\
&\equiv \mathsf{T} \vee \mathsf{T} \quad \text{Becouse of} \quad \neg p \vee p \equiv \mathsf{T} \\
&\equiv \mathsf{T}
\end{aligned}$$

Try to verify the above tautologies using the logic equivalence laws.

For logic equivalence laws in Wiki, see `https://en.wikipedia.org/wiki/Logical_equivalence`. In addition to many, there is a nice webpage with a video for logical equivalence with 13 examples, see `https://calcworkshop.com/logic/logical-equivalence/`.

Answer :

- $\neg p \wedge (p \vee q) \rightarrow q$.

$$\begin{aligned}
\neg p \wedge (p \vee q) \rightarrow q &\equiv \neg(\neg p \wedge (p \vee q)) \vee q \\
&\equiv p \vee \neg(p \vee q) \vee q) \\
&\equiv (p \vee (\neg p \vee \neg q)) \vee q \quad \text{De Morgan} \\
&\equiv (p \vee \neg p) \wedge (p \vee \neg q) \vee q \\
&\equiv \mathsf{T} \wedge (p \vee q) \vee q \quad \text{Because of} \quad p \vee \neg p \equiv \mathsf{T} \\
&\equiv p \vee (q \vee q) \\
&\equiv p \vee \mathsf{T} \quad \text{Because of} \quad q \vee \neg q \equiv \mathsf{T} \\
&\equiv \mathsf{T}
\end{aligned}$$

- $(p \wedge q) \rightarrow r \Leftrightarrow p \rightarrow (q \rightarrow r)$.

$$\begin{aligned}(p \wedge q) \rightarrow r &\equiv \neg(p \wedge q) \vee r \\ &\equiv (\neg p \vee \neg q) \vee r \quad \text{De Morgan} \\ &\equiv \neg p \vee (\neg q \vee r) \\ &\equiv \neg p \vee (q \rightarrow r) \\ &\equiv p \rightarrow (q \rightarrow r)\end{aligned}$$

$$\begin{aligned}p \rightarrow (q \rightarrow r) &\equiv \neg p \vee (\neg q \vee r) \\ &\equiv (\neg p \vee \neg q) \vee r \\ &\equiv \neg(p \wedge q) \vee r \quad \text{De Morgan} \\ &\equiv (p \wedge q) \rightarrow r\end{aligned}$$

- $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow [p \rightarrow r]$

$$\begin{aligned}[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow [p \rightarrow r] &\equiv [(\neg p \vee q) \wedge (\neg q \vee r)] \rightarrow [\neg p \vee r] \\ &\equiv \neg(\neg p \vee q) \vee \neg(\neg q \vee r) \vee (\neg p \vee r) \quad \text{De Morgan} \\ &\equiv (p \wedge \neg q) \vee (q \wedge \neg r) \vee \neg p \vee r \\ &\equiv \neg p \vee (p \wedge \neg q) \vee (q \wedge \neg r) \vee r \quad \text{Commutativity and Associativity} \\ &\equiv [(\neg p \vee p) \wedge (\neg p \vee \neg q)] \vee [(q \vee r) \wedge (\neg r \vee r)] \\ &\equiv [\mathsf{T} \wedge (\neg p \vee \neg q)] \vee [(q \vee r) \wedge \mathsf{T}] \\ &\equiv (\neg p \vee \neg q) \vee (q \vee r) \\ &\equiv \neg p \vee \neg q \vee q \vee r \\ &\equiv \neg p \vee \mathsf{T} \vee r \\ &\equiv \mathsf{T}\end{aligned}$$

9 Propose a logical implication formula for the statement $x \leq y$.

Logical implication is a type of relationship between two statements or sentences. Even for a single mathematical statement, there exists implicit logical implication among its variables (arguments). The relation translates verbally into "logically implies" or the logical connective "if/then" and is symbolized by a double-lined arrow pointing toward the right $\Longrightarrow$

In logic, implication is the relationship between different propositions where the second proposition is a logical consequence of the first. For instance, if A and B represent semantic statements, then $A \Longrightarrow B$ means "A implies B" or "If A, then B." The word "implies" is used in the strongest possible sense.

Question: Propose a logical implication formula for the statement $x \leq y$ (suppose that x and y are real numbers). Moreover, from this example, we will explore the equivalence of the two logical formulas $P \vee Q$ and $\neg P \Longrightarrow Q$ by a gut feeling.

Answer :

The logical implication formula for the statement **"**$x \leq y$**"** is:

$x \leq y \Rightarrow True$

This formula states that if "x is less than or equal to y," then the implication is True. In other words, if the condition **"**$x \leq y$**"** is met, then the implication is always True, indicating that the statement **"**$x \leq y$**"** is satisfied.

Now, let's explore the equivalence of the two logical formulas:

$$P \vee Q$$
$$\neg P \Rightarrow Q$$

The formula $P \vee Q$ represents a logical "or" statement, meaning it is True if either P or Q is True (or both). In other words, it allows for multiple possibilities, and it's True as long as at least one of the conditions P or Q is satisfied.

The formula $\neg P \Rightarrow Q$ represents a logical implication. It states that if P is not True ($\not P$) then Q must be True. In this case, it's a conditional statement, and it implies that if the condition P is not met, then the condition Q must be met.

These two formulas are not equivalent. The key difference is that in the first formula ($P \vee Q$), you have the flexibility that either P or Q (or both) can be True to make the statement True. In the second formula ($\neg P \longrightarrow Q$), it specifically states that if P is not True, then Q must be True for the implication to be satisfied.

For example, let's use P to represent "It is raining" and Q to represent "I carry an umbrella."

- The formula $P \vee Q$ means that if it's either raining or I carry an umbrella, the statement is True. This allows for the possibility that I might carry an umbrella even when it's not raining.
- The formula $\neg P \Rightarrow Q$ means that if it's not raining, then I must carry an umbrella. This is a stronger condition, as it implies that the only situation where I would carry an umbrella is when it's not raining.

So, while these two logical formulas are related, they have different meanings and do not represent the same concept.

10 Use predicate logic to express Goldbach's weak conjecture and Chen's theorem

Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states that every even whole number greater than 2 is the sum of two prime numbers. The conjecture was first proposed in a letter from Christian Goldbach(1690-1764, German mathematician) to Leonhard Euler (1707-1783, Swiss mathematician, physicist, astronomer, geographer, logician, and engineer who founded the studies of graph theory and topology and made pioneering and influential discoveries in many other branches of mathematics such as analytic number theory, complex analysis, and infinitesimal calculus. He introduced much of modern mathematical terminology and notation. He is also known for his work in mechanics, fluid dynamics, optics, astronomy, and music theory) on 7 June 1742. A modern version of Goldbach's conjecture of which Euler reminded him is:

Every even integer greater than 2 can be written as the sum of two primes.

Keeping in mind that $\mathbb{N}$ denotes the set of natural numbers, Goldbach's conjecture can be written as the following formula in predicate logic:

$$\begin{aligned}[(\forall k \in \mathbb{N})x = 2k]\&[x > 2] \Rightarrow &[(\exists y_1 \in \mathbb{N})(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})y_1 = mn \longrightarrow (m = 1) \vee (n = 1)]\& \\ &[(\exists y_2 \in \mathbb{N})(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})y_2 = mn \longrightarrow (m = 1) \vee (n = 1)]\& \\ &[x = y_1 + y_2]\end{aligned}$$

A weaker form of Goldbach's conjecture, known as "Goldbach's weak conjecture", asserts that

Every odd integer greater than 7 can be written as the sum of three odd primes.

The best result regarding Goldbach's conjecture so far is from Jingrun Chen (1933-1996, a Chinese mathematician focusing on the analytical number theory), known as Chen's theorem first proved in 1966 and then expanded in 1970. It says

Every sufficiently large even number can be written as the sum of a prime and a semiprime (the product of two primes).

Use predicate logic to express Goldbach's weak conjecture and Chen's theorem.

Example: The statement that any non-zero real number has a reciprocal can be expressed as a formula in predicate logic:
$[(\forall x \in \mathbb{R})x \neq 0] \Rightarrow [(\exists y \in \mathbb{R})xy = 1]$.

Example: Given two sets A and B, A is said to be a subset of B if any element in A belongs to B. This definition can be equivalently expressed as a formula in predicate logic:
$A \subseteq B \stackrel{def}{=} [(\forall x)x \in A] \Rightarrow [x \in B]$.

Example: For any prime p, $\sqrt{p}$ is irrational. This fact can be represented as the following predicate logic formula.
$[(\forall p \in \mathbb{N})(\nexists m, n \in mathbbN \setminus \{1, p\})p = mn] \Rightarrow [(\nexists a, b \in \mathbb{N})b \neq 0 \wedge \sqrt{p} = \frac{a}{b}]$.

Question: Between any two rational numbers $a < b$, there is an irrational number. This fact can be represented as the following predicate logic formula:
$(\forall a, b \in \mathbb{Q})(\exists x \notin \mathbb{Q})a < x < b$.
Show the above predicate is true (referring to textbooks on Real Analysis).

Remark: Given a number x, the fact that it is a prime can be represented as the following predicate:
$\forall y(y < x \Rightarrow (y = 1 \vee \neg(div(y, x)))$.
where div(y, x) is true if y divides x.

Answer :

$$\forall y(y < x \Rightarrow (y = 1 \vee \neg(div(y, x))) \Rightarrow \forall y(y < x \Rightarrow (y = 1 \vee \neg(div(y, x)))$$

1. Let a and b be two rational numbers such that $a < b$. We aim to find an irrational number x such that $a < x < b$.
2. We can construct the following Diophantine equation to find such x:

$n(a - x) = x - m(b - a)$
where n and m are integers, and both n and m are not zero.

4. The purpose of this equation is to find a number x that lies between a and b and is an irrational number.
5. Now, we can rearrange the equation as follows:

$x = \frac{na+mb}{n+m}$

6. This equation suggests that x can be represented as a ratio of integers n and m, making x a rational number.
7. However, we can adjust the values of n and m in such a way that the numerator $na + mb$ cannot be simplified, resulting in x being an irrational number.
8. Therefore, we must select values for n and m to ensure that $na + mb$ cannot be reduced to a simpler fraction.
9. By choosing appropriate values for n and m, we can ensure that x is an irrational number and it falls between a and b.
10. This concludes our proof. We have successfully found an irrational number x such that $a < x < b$.
11. Furthermore, according to the premise that $a < x$, we can draw the following conclusion:

$\forall y, (y < x \Rightarrow (y = 1 \vee \neg\,(\mathrm{div}(y, x))))$
This is because, for any y, if y is less than x, then y must either equal 1 or not be divisible by x.

11 Propose a predicate for Well-Ordering Principle.

Given an alphabet Σ, $L \subseteq \Sigma^*$ is said to be a language defined over Σ. A language L is called a regular language if it is recognized (or accepted) by a deterministic finite automaton (DFA) or a non-deterministic finite automaton (NFA); this implies that DFAs and NFAs have the same modeling power. A regular language has a nice property called the Pumping Lemma. Again, the pumping lemma is a property of a regular language. It is used to prove the non-regularity of certain languages. Regular languages always satisfy the pumping lemma. However, if the pumping lemma is satisfied, the language does not need to be regular. It is worth mentioning that this is only useful for infinite languages since all finite languages are regular.

The Pumping Lemma is useful for disproving the regularity of a specific language in question. It was first proven by Michael Rabin (1928-, an Israeli mathematician and computer scientist) and Dana Scott (1932-, an American logician) in 1959. In 1976, the Turing Award was awarded jointly to M. Rabin and D. Scott for a paper written in 1959, the citation for which states that the award was granted:

For their joint paper "Finite Automata and Their Decision Problems," which introduced the idea of nondeterministic machines, which has proved to be an enormously valuable concept. Their (Scott & Rabin) classic paper has been a continuous source of inspiration for subsequent work in this field.

Pumping Lemma: Let L be a regular language. There exists a number $p \in \mathbb{N}$ such that for any $s \in L$ with $|s| \geq p$, s can be divided into three pieces, $s = xyz$, satisfying

- $xy^iz \in L$ for all $i \geq 0$,
- $|y| \geq 1$,i.e.,$y \neq \epsilon$,
- $|xy| \leq p$

The pumping lemma can be expressed as the predicate

$$(\forall s \in L)(\exists p \in \mathbb{N})\,|s| \geq p \Longrightarrow [(\exists x, y, z \in \Sigma^*)s = xyz] \wedge [(\forall i \in \mathbb{N})xy_iz \in L] \wedge [|y| \geq 1] \wedge [|xy| \leq p]$$

Question: Propose a predicate for Well-Ordering Principle. In mathematics, the well-ordering principle states that every non-empty set of positive integers contains a least element. In other words, the set of positive integers is well-ordered by its "natural" or "magnitude" order in which x precedes y if and only if y is either x or the sum of x and some positive integer. The phrase "well-ordering principle" is sometimes taken to be synonymous with the "wellordering theorem". On other occasions, it is understood to be the proposition that the set of integers {. . . , -2, -1, 0, 1, 2, 3, . . .} contains a well-ordered subset, called the natural numbers, in which every non-empty subset contains a least element.

Depending on the framework in which the natural numbers are introduced, this property of the set of natural numbers is either an axiom or a provable theorem.
The well-ordering principle seems sort of obvious. However, it requires a nonempty set—it is false for the empty set which has no smallest element because it has no elements at all. Further, it requires a set of nonnegative integers—it is false for the set of negative integers and also false for some sets of nonnegative rationals, for example, the set of positive rationals. Actually, the well-ordering principle captures something special about the nonnegative integers. While the well-ordering principle may seem obvious, it in fact provides one of the most important proof rules in discrete mathematics.
In most cases, we actually have already taken this property for granted. For example, in proving that $\sqrt{2}$ is irrational, we naturally assume that for any positive integers $m\prime$ and $n\prime$, the fraction $m\prime/n\prime$ can be written in lowest terms, that is, in the form m/n, where m and n are positive integers with no common prime factors.

Answer :

$$[S\prime = \{a_1, a_2, a_3, ...a_{k+1}\}S\prime \subset \mathbb{Z}^+][(x \in S\prime)(\forall y \in S\prime))][(x < y) \vee (y \leq x)] \Rightarrow (\forall S \in \mathbb{Z}^+) \wedge (S \neq \Phi) \wedge (\exists x \in S)(\forall y \in S)x < y$$

Consider a non-empty set S' containing $k+1$ positive integers. We need to show that it also contains a least element. Let S_1 be a subset of S' containing k positive integers, and let x be the $(k+1)$-th element in S'. According to our inductive hypothesis, the set S_1 has a least element, denoted as y.

Now, compare y and x:

- If $y \leq x$, then y is the least element in S'.
- If $x < y$, then x is the least element in S'.

In either case, S' contains a least element.

12 Order of forall and exists

When quantifiers in the same predicate are of the same quantity (all universal or all existential), the order in which they occur does not matter. However, when they are mixed, the order in which they occur becomes crucial. Consider the following examples:

$$\forall x \forall y.\text{Likes}(x, y) \Leftrightarrow \forall y \forall x.\text{Likes}(x, y), \text{ and} \exists x \exists y.\text{Likes}(x, y) \Leftrightarrow \exists y \exists x.\text{Likes}(x, y)$$

These are clearly equivalent pairs. The first pair contains two different ways of saying everyone likes everyone. The second contains two different ways of saying someone likes someone.

Now consider this mixed quantifier case:

$$\forall x \exists y.\text{Likes}(x, y) \not\Leftrightarrow \forall y \exists x.\text{Likes}(x, y)$$

Clearly, the two predicates are not equivalent. The one on the left says (very plausibly) that everyone likes someone (or another), but allows for the possibility that different people have different likes-I like Martinez, you like Griffey, Madonna likes herself, etc. The one on the right, however, says something much stronger-it says that there is at least one person so well-liked that everyone likes him or her. (It is very unlikely that there is such a person, and so very unlikely that the predicate on the right is true.)

Notice that the stronger predicate (on the right) logically implies the weaker one (on the left). In general, an $\exists\forall$ predicate logically implies its $\forall\exists$ counterpart, but not conversely.

Question: Plausibly, an $\exists\forall$ predicate logically implies its $\forall\exists$ counterpart. Elaborate upon in plain words the correctness of the above reasoning.
Let us first consider a more dramatic contrast with the following two predicates:

$$\forall x\exists y(x = y) \nLeftrightarrow \forall y\exists x(x = y)$$

Remark: There exists a number of different ways to capture the difference between the two predicates $\forall x\exists y.P(x, y)$ and $\exists y\forall x.P(x, y)$. From the computational viewpoint, the former corresponds to the problem verification and the latter corresponds to the problem solution. In other words, $\forall x\exists y.P(x, y)$ means that given a certificate (solution) y, we are going to verify whether $P(x, y)$ is true, while $\exists y\forall x.P(x, y)$ implies that given a problem y, we have to find a solution x such that $P(x, y)$ is true. The latter is obviously harder in computation and stronger in logic than the former.

Remark: An exact and precise understanding of logic formulas is crucial. For example, the truth of $P \vee Q$ means that at least one of P and Q is true. Keeping this in mind, it is ready for us to observe the equivalence of $P \vee Q$ and $\neg(\neg P \wedge \neg Q)$. From this formula, we could see that logic OR can be defined by "not" and "and". Actually, in proposition logic, only $\neg$ and $\wedge$ are primitives, while other connectives like $\Longrightarrow$, $\vee$, and $\nLeftrightarrow$ can be defined by the two primitive connectives.

Answer :

- $\forall x\exists y(x = y)$: This predicate states that for every element x, there exists another element y such that x equals y. In plain words, it means that everything is equal to something.
- $\exists y\forall x(x = y)$: This predicate states that there exists an element y such that for all elements x, x equals y. In plain words, it means that there's a single element that is equal to everything.

These two predicates are not equivalent. The first one allows for each element to have its unique counterpart, while the second one implies that there's a universal element that is equal to everything, which might not be the case. The second predicate is stronger in its assertion and is not equivalent to the first one. It's an example of how the order of quantifiers matters in predicate logic.

13 Suppose that an alphabet

Suppose that an alphabet Σ is finite. Show that Σ^* is countable (hint: consider Cantor's diagonal argument by the lengths of the strings in Σ^*. Specifically, enumerate in the first row the string whose length is zero, in the second row the strings whose lengths are one, and so on).

From time to time, we mention the terminology *strings, finite strings*, and *infinite strings*. Formally, a finite sequence of symbols (called a string in most cases) over an alphabet Σ (usually finite) is a mapping $s : \{1, 2, ..., n\} \to \Sigma$, denoted by the string $\sigma_1\sigma_2 \cdots \sigma_n$, where $\sigma_i = s(i) \in \Sigma$ for every $1 \leq i \leq n$, or the mapping $\epsilon : \Theta \to \Sigma$, the empty sequence. An infinite sequence is a mapping s : $\mathbb{N} \to \Sigma$. We write $s = \sigma_1\sigma_2\Sigma_3 \cdots$ with $\sigma(i) = s(i) \in \Sigma$.

Answer :

1. consider strings of length zero in Σ^*. There is only one empty string ϵ.
2. consider strings of length one in Σ^*. Since Σ is finite, there are a finite number of choices for each character in the string. Let's say there are m characters in Σ. So, there are m strings of length one: $\sigma_1, \sigma_2, ..., \sigma_m$.
3. For strings of length two, we can have m^2 possible strings. Enumerate them as $\sigma_1\sigma_1, \sigma_2\sigma_2, ..., \sigma_1\sigma_m, \sigma_2\sigma_1, \sigma_2\sigma_2, ..., \sigma_m\sigma_m$
4. Continue this process for strings of length three, four, and so on. For strings of length n, there are m^n possibilities.

Length 0	ϵ
Length 1	$\sigma_1, \sigma_2, ..., \sigma_m$
Length 2	$\sigma_1\sigma_1, \sigma_2\sigma_2, ..., \sigma_1\sigma_m, \sigma_2\sigma_1, \sigma_2\sigma_2, ..., \sigma_m\sigma_m$
Length 3	$\cdots$
Length 4	$\cdots$
...	$\cdots$

Now, to prove that Σ^* is countable, we can arrange all these strings in a table:

This enumeration covers all possible strings in Σ^*, organized by their lengths. Each cell in the table corresponds to a unique string in Σ^*.

Since each row represents a finite set (the set of strings of a particular length), and there are countably many rows (one row for each non-negative integer), we can apply the countable union of countable sets principle to conclude that the set Σ^* is countable.

14 * The set of polynomials with integer coefficients is countable.

Answer :

Here's a more detailed explanation of the argument:

- Each polynomial with integer coefficients can be represented as a finite sequence of its coefficients. For example, the polynomial:

  $P(x) = 3x^2 - 2x + 1$

  can be represented as the sequence of coefficients: [3, -2, 1].

- Since each coefficient is an integer, each element of the sequence is an element of the countable set of integers.

- The set of all finite sequences of integers is countable because it can be put into one-to-one correspondence with the set of natural numbers (positive integers). This can be done by considering sequences of length 1, length 2, length 3, and so on, and ordering them in a systematic way.

- Therefore, since we can map each polynomial with integer coefficients to a finite sequence of integers, and the set of finite sequences of integers is countable, the set of polynomials with integer coefficients is also countable.

In summary, the set of polynomials with integer coefficients is countable because it can be put into a one-to-one correspondence with the countable set of all finite sequences of integers, which can be systematically ordered and enumerated.

15 * A complex number x is said to be algebraic if there are integers $a_0, a_1, ..., a_n$, not all zero, such that $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$. Prove that the set of all algebraic numbers is countable.

Answer :

Proof:

- Consider the set of all polynomials with integer coefficients. Each polynomial can be represented as:

  $P(x) = a_n x^n + a_{n-1}x^(n-1) + ... + a_1 * x + a_0$

  where a0, a1, ..., an are integers, and not all of them are zero.

- For each polynomial P(x), let's consider the set of its roots (solutions) in the complex numbers. These roots are the algebraic numbers associated with this polynomial.

- Now, for each polynomial P(x), the set of its roots is a finite set of complex numbers. These roots satisfy the polynomial equation P(x) = 0.

- We can define a mapping that associates each polynomial P(x) to its set of roots. In other words, we can create a function f(P) that takes a polynomial as input and outputs the set of roots for that polynomial.

- The number of such polynomials with integer coefficients is countable because the set of all finite sequences of integers is countable (as explained in a previous response).

- For each polynomial, the set of its roots is finite, and the union of countably many finite sets is still countable.
- Therefore, the set of algebraic numbers, which is the union of the sets of roots for all possible polynomials with integer coefficients, is also countable.

In conclusion, the set of algebraic numbers is countable because it can be shown that there are countably many polynomials with integer coefficients, and the set of algebraic numbers is a countable union of the finite sets of roots associated with these polynomials.

16 Let $\Sigma = \{0, 1\}$, $A = \{\omega \in \Sigma^* | \omega$ has the equal number of 01$\}$, and $B = \{0^*1^*\} = 0^m1^n | m \geq 0, n \geq 0$. Write the expression of $A \cap B$.

Answer :

Write the expression for the intersection ($A \cap B$) of the two languages A and B, need to find the strings that belong to both A and B. In this case, A represents strings with an equal number of '0's and '1's, and B represents strings that are in the form of 0^m1^n, where m and n can be any non-negative integers.

The intersection $A \cap B$ will contain strings that satisfy both conditions, i.e., strings that have an equal number of '0's and '1's and are in the form of 0^m1^n. The only string that satisfies both conditions is the empty string ϵ, as it has an equal number of '0's and '1's (zero each) and is also in the form 0^m1^n for m = 0 and n = 0.

So, the expression is:

$A \cap B = \{\epsilon\}$

In this case, the intersection of languages A and B contains only the empty string.

17 *Mathematical proof

* (Mathematical proof) A mathematical proof is an inferential argument for a mathematical statement, showing that the stated assumptions logically guarantee the conclusion. The argument may use other previously established statements, such as theorems; but every proof can, in principle, be constructed using only certain basic or original assumptions known as axioms along with the accepted rules of inference. Proofs are examples of exhaustive deductive reasoning, which establish logical certainty, to be distinguished from empirical arguments or non-exhaustive inductive reasoning which establishes reasonable expectation. Presenting many cases in which the statement holds is not enough for proof, which must demonstrate that the statement is true for all possible cases. A proposition that has not been proved but is believed to be true is known as a conjecture, or a hypothesis if frequently used as an assumption for further mathematical work.

Proofs employ logic expressed in mathematical symbols, along with natural language which usually admits some ambiguity. In most mathematical literature, proofs are written in terms of rigorous informal logic. Purely formal proofs, written fully in a symbolic language without the involvement of natural language, are considered in proof theory. The distinction between formal and informal proofs has led to much examination of current and historical mathematical practice, quasi-empiricism in mathematics, and so-called folk mathematics, oral traditions in the mainstream mathematical community or in other cultures. The philosophy of mathematics is concerned with the role of language and logic in proofs, and mathematics as a language.

There is a book entitled "Book of Proof" by Professor Richard Hammack, which is free-downloadable. More books on mathematical proofs (as well as those on other mathematical disciplines) can be found on the website of American Institute of Mathematics' Open Textbook Initiative.

This book is an introduction to the language and standard proof methods of mathematics. It is a bridge from the computational courses (such as calculus or differential equations) that students typically encounter in their first year of college to a more abstract outlook. It lays a foundation for more theoretical courses such as topology, analysis and abstract algebra. Although it may be more meaningful to the student who has had some calculus, there is really no prerequisite other than a measure of mathematical maturity.

The book "How to Read and Do Proofs: An Introduction to Mathematical Thought Processes," (6th Edition) by Professor Daniel Solow, Department of Operations, Weatherhead School of Management, Case Western Reserve University, is designed to reduce the time and frustration involved in learning how to read, think about, understand, and "do" mathematical proofs and also to provide a description of other mathematical "thinking processes". It is suitable as a text for an undergraduate transition-to-advanced-math course, as a supplement to any course involving proofs, or for self-guided reading (especially for Ph.D. students in mathrelated areas such as Statistics, Computer Science, Physics, Engineering, Finance, Economics, and Business). Here are the videos of the book.

In addition, a noted textbook: Mathematical Proofs: A Transition to Advanced Mathematics by G. Chartrand, A. D. Polimeni, and P. Zhang is highly recommended.

X	C	$\neg X$	$\neg X \Rightarrow C$	$[\neg X \Rightarrow C] \Rightarrow X$
T	F	F	T	T
F	F	T	F	T

P	Q	$\neg P$	$\neg Q$	$p \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

18 Proof by contrapositive

(Methods of proof) Typical mathematical proof methods include Direct proof, Proof by mathematical induction, Proof by contrapositive, Proof by contradiction, Proof by construction, Proof by exhaustion, Probabilistic proof, Combinatorial proof, Nonconstructive proof, Statistical proof in pure mathematics, and Computerassisted proof. Here we focus on the proofs by contradiction and by contrapositive. As defined, a tautology is usually a compound statement that is true for all possible combinations of truth values of the component statements that are part of the statement. A contradiction is a compound statement that is false for all possible combinations of truth values of the component statements that are part of the statement. That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

Proof by contradiction is frequently used in mathematical proof. This method is based on the fact that a statement X can only be true or false (and not both). The idea is to prove that the statement X is true by showing that it cannot be false. This is done by assuming that X is false and proving that this leads to a contradiction. (The contradiction often has the form $Q \wedge \neg Q$, where Q is some statement.) When this happens, we can conclude that the assumption that the statement X is false is incorrect, and hence X cannot be false. Since it cannot be false, then X must be true.

A logical basis for the contradiction method of proof is the tautology

$$[\neg X \Rightarrow C] \Rightarrow X$$

where X is a statement and C is a contradiction. The following truth table establishes this tautology.

This tautology shows that if $\neg X$ leads to a contradiction, then X must be true. The previous truth table also shows that the statement $\neg X \Rightarrow C$ is logically equivalent to X. This means that if we have proved that $\neg X$ leads to a contradiction, then we have proved statement X. So if we want to prove a statement X using a proof by contradiction, we assume that $\neg X$ is true and show that this leads to a contradiction.

Question: Show by contradiction that for all real numbers x and y, if $x \neq y, x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.
Hint: consider a contradiction $[(\forall x, y \in \mathbb{R})(x-y)^2 \geq 0] \wedge [(\forall X, y \in \mathbb{R})(x-y)^2 < 0)]$.

In logic, the contrapositive of a conditional statement is formed by negating both terms and reversing the direction of inference. Proof by contrapositive takes actually advantage of the logical equivalence between "P implies Q" and "Not Q implies Not P ". For example, the assertion "If it is my car, then it is red" is equivalent to "If that car is not red, then it is not mine". Thus, to prove "If P , Then Q" by the method of contrapositive means to prove "If Not Q, Then Not P ".

Although it is possible to use direct proof exclusively, there are occasions where contrapositive proof is much easier. The difference between the Contrapositive method and the Contradiction method is subtle. Let us examine how the two methods work when trying to prove "If P , Then Q".

- Method of Contradiction: Assume P and Not Q and prove some sort of contradiction.
- Method of Contrapositive: Assume Not Q and prove Not P .
- The method of Contrapositive has the advantage that your goal is clear: Prove Not P . In the method of Contradiction, your goal is to prove a contradiction, but it is not always clear what the contradiction is going to be at the start.

According to the table, statements $P \Rightarrow Q$ and $\neg Q \Rightarrow lnotP$ are different ways of expressing exactly the same thing. The expression $\neg Q \Rightarrow \neg P$ is called the contrapositive form of $P \Rightarrow Q$. We outline for Contrapositive Proof as follows.

Proposition If P, then Q.
Proof : Suppose $\neg Q$.
vdots
Therefore, $\neg P$, which completes the proof.

As seen, the setup for contrapositive proof is very simple. The first line of the proof is the sentence "Suppose that Q is not true." The last line is the sentence "Therefore P is not true, which completes the proof." Between the first and last line, we use logic and definitions to transform the statement $\neg Q$ to the statement $\neg P$. To illustrate this new technique, and to contrast it with direct proof, we now prove a proposition in two ways: first with direct proof and then with contrapositive proof.

Question Show by contrapositive the following result:
If $x^2 - 6x + 5$ is even, then x is odd.
Furthermore, propose a direct proof method and compare the two methods for this specific example.

Remark: A direct proof would be problematic. We would begin by assuming that x^2-6x+5 is even, so $x^2-6x+5 = 2a$ for some integer a. Then we would need to transform this into $x = 2b + 1$ for $b \in \mathbb{Z}$. However, it is not quite clear how that could be done, for it would involve isolating an x from the quadratic expression. The proof becomes very simple if we use contrapositive proof.

Question Let $f(x)$ be a real polynomial function such that $f(2x) = f\prime(x)f\prime\prime(x)$. Show by contrapositive that the degree of $f(x)$ is not four.
Hint: An n-degree polynomial takes the form $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, where $n \in \mathbb{N}$ is a non-negative integer.

Answer :

A1 :
$(\frac{x}{y} + \frac{y}{x} > 2)(x, y \in \mathbb{R})x \neq y, x > 0, y > 0,$

1. We assume the opposite, which is that there exist real numbers x and y such that $x \neq y$, $x > 0$, $y > 0$, and $\frac{x}{y} + \frac{y}{x} \leq 2$.
2. We then consider the expression $(x - y)^2$. Since $x, y \in \mathbb{R}$ and $x \neq y$, $(x - y)^2 > 0$.
3. Now, we consider the expression $\frac{x}{y} + \frac{y}{x} - 2$, which is the same as $\frac{x^2+y^2-2xy}{xy}$.
4. We have assumed that $\frac{x}{y} + \frac{y}{x} \leq 2$, which means $\frac{x^2+y^2-2xy}{xy} \leq 2$.
5. Rearrange the above inequality: $x^2 + y^2 - 2xy \leq 2xy$.
6. Simplify further: $x^2 + y^2 \leq 4xy$.
7. Divide both sides by xy: $\frac{x}{y} + \frac{y}{x} \leq 4$.

Now, we have a contradiction. We assumed that $\frac{x}{y} + \frac{y}{x} \leq 2$ and arrived at $\frac{x}{y} + \frac{y}{x} \leq 4$, which is a contradiction.
Since our initial assumption led to a contradiction, we conclude that the original statement is true: For $x, y \in \mathbb{R}$, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

A2 :
We assume the opposite, which is that if $x^2 - 6x + 5$ is even, x is not necessarily odd.

1. Let's assume that if $x^2 - 6x + 5$ is even, x can be either even or odd. In other words, we assume that x can be expressed as $x = 2k$ or $x = 2k + 1$, where $k \in \mathbb{Z}$.
2. We then calculate $x^2 - 6x + 5$:
   $x^2 - 6x + 5 = (2k)^2 - 6(2k) + 5 = 4k^2 - 12k + 5 = 4(k^2 - 3k) + 5$

3. Since $k \in \mathbb{Z}$, $k^2 - 3k \in \mathbb{Z}$, and $4(k^2 - 3k)$ is a multiple of 4. Adding 5 to a multiple of 4 results in an integer, which means that $x^2 - 6x + 5$ is an odd number.

4. We have reached a contradiction. Our initial assumption stated that if $x^2 - 6x + 5$ is even, x can be either even or odd. However, our calculation showed that $x^2 - 6x + 5$ is an odd number, which contradicts the assumption.

Since our initial assumption leads to a contradiction, we conclude that the original statement is true: If $x^2 - 6x + 5$ is even, then x is indeed an odd number.

A3 :

We want to prove that if the degree of $f(x)$ is four, then $f(2x) \neq f\prime(x)f\prime\prime(x)$. This is the contrapositive of the given statement.

1. Let $f(x)$ be a polynomial of degree four:
   $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$

2. Now, let's consider $f(2x)$:
   $f(2x) = a_4(2x)^4 + a_3(2x)^3 + a_2(2x)^2 + a_1(2x) + a_0$

3. Simplify this expression:
   $f(2x) = 16a_4x^4 + 8a_3x^3 + 4a_2x^2 + 2a_1x + a_0$

4. Next, we consider $f\prime(x)$ and $f\prime\prime(x)$. The derivatives are as follows:
   $f\prime(x) = 4a_4x^3 + 3a_3x^2 + 2a_2x + a_1$
   $f\prime\prime(x) = 12a_4x^2 + 6a_3x + 2a_2$

5. Now, we calculate $f\prime(x)f\prime\prime(x)$:
   $f\prime(x)f\prime\prime(x) = (4a_4x^3 + 3a_3x^2 + 2a_2x + a_1)(12a_4x^2 + 6a_3x + 2a_2)$

6. Multiplying these polynomials:
   $f\prime(x)f\prime\prime(x) = 48a_4x^5 + 30a_3x^4 + (24a_4a_2 + 18a_3a_2)x^3 + (16a_4a_1 + 12a_3a_1 + 12a_2^2)x^2 + 6a_2a_1x$

7. Now, we have the expressions for $f(2x)$ and $f\prime(x)f\prime\prime(x)$:
   $f(2x) = 16a_4x^4 + 8a_3x^3 + 4a_2x^2 + 2a_1x + a_0$
   $f\prime(x)f\prime\prime(x) = 48a_4x^5 + 30a_3x^4 + (24a_4a_2 + 18a_3a_2)x^3 + (16a_4a_1 + 12a_3a_1 + 12a_2^2)x^2 + 6a_2a_1x$

8. Now, let's examine the degree of both polynomials:

   The degree of $f(2x)$ is 4.

   The degree of $f\prime(x)f\prime\prime(x)$ is 5.

   Since the degree of $f(2x)$ is not equal to the degree of $f\prime(x)f\prime\prime(x)$, we have shown that if the degree of $f(x)$ is four, then $f(2x)$ is not equal to $f\prime(x)f\prime\prime(x)$.

Therefore, we have proved by contrapositive that the degree of $f(x)$ is not four.

19 Group is an elementary notion in algebra

Group is an elementary notion in algebra, which refers generally to a set with a binary operation regarding its elements and a special element in the set. As a special group, a monoid is a triple $(X, \square, i)$ consisting of a set X, a binary operation $\square$, and a special element $i \in X$ (called the identity element of X), satisfying the following rules:

$$\begin{cases} (x\square y)\square z = x\square(y\square z) & \text{(associative law)} \\ \square i = i\square x & \text{(identity law)} \end{cases}$$

for all $x, y, z \in X$. The fundamental operations of the monoid are $\square$ (binary) and i (nullary). We may refer to X itself as a monoid if i and $\square$ do not need to be specified explicitly. Given a monoid $(X, \square, i)$, X is called the underlying set of the monoid.

Question 1. Let Σ be an alphabet and $\epsilon \in \Sigma^*$ be the empty string. Show that (Σ^*, o, ϵ) is a monoid, where o is the concatenation operation of strings.

Further reading: In abstract algebra, group theory studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces, can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have influenced many parts of algebra. Linear algebraic groups and Lie groups are two branches of group theory that have experienced advances and have become subject areas in their own right.

In mathematics, a group is a set equipped with an operation that combines any two elements of the set to produce a third element of the set, in such a way that the operation is associative, an identity element exists and every element has an inverse. These three conditions, called group axioms, hold for number systems and many other mathematical structures. For example, the integers together with the addition operation form a group. The concept of a group and its definition through the group axioms was elaborated for handling, in a unified way, essential structural properties of entities of very different mathematical nature (such as numbers, geometric shapes and polynomial roots). Because of the ubiquity of groups in numerous areas (both within and outside mathematics), some authors consider them as a central organizing principle of contemporary mathematics.

Groups arise naturally in geometry for the study of symmetries and geometric transformations: the symmetries of an object form a group, called the symmetry group of the object, and the transformations of a given type form generally a group. Lie groups arise as symmetry groups in geometry but appear also in the Standard Model of particle physics. The Poincaré (1854-1912, French mathematician, theoretical physicist, engineer, and philosopher of science) group is a Lie group consisting of the symmetries of spacetime in special relativity. Point groups describe symmetry in molecular chemistry.
The concept of a group arose from the study of polynomial equations, starting with Évariste Galois (1811-1832, French mathematician) in the 1830s, who introduced the term group (groupe, in French) for the symmetry group of the roots of an equation, now called a Galois group. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—an active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups.

In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely, both from a point of view of representation theory (that is, through the representations of the group) and of computational group theory. A theory has been developed for finite groups, which culminated with the classification of finite simple groups, completed in 2004. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become an active area in group theory (from `https://en.wikipedia.org/wiki/Group_(mathematics)`).

Example 1. One of the more familiar groups is the set of integers $\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$ together with addition.

For any two integers a and b, the sum $a + b$ is also an integer; this closure property says that "+" is a binary operation on $\mathbb{Z}$. The following properties of integer addition serve as a model for the group axioms in the definition below.

For all integers a, b, and c, one has $(a + b) + c = a + (b + c)$. Expressed in words, adding a to b first, and then adding the result to c gives the same final result as adding a to the sum of b and c. This property is known as associativity.

If a is any integer, then $0 + a = a$ and $a + 0 = a$. Zero is called the identity element of addition because adding it to any integer returns the same integer. For every integer a, there is an integer b such that $a + b = 0$ and $b + a = 0$. The integer b is called the inverse element of the integer a, denoted $-a$. The integers, together with the operation +, form a mathematical object belonging to a broad class sharing similar structural aspects. To appropriately understand these structures as a collective, the following definition is developed.

Formally, a group is a set G together with a binary operation on G, here denoted by "$\cdot$", that combines any two elements a and b to form an element of G, denoted by ab, such that the following three requirements, known as group axioms, are satisfied:

- **Associativity:** For all a, b, c in G, one has $(ab)c = a(bc)$.
- **Identity element:** There exists an element e in G such that, for every a in G, one has $ea = a$ and $ae = a$. Such an element is unique, called the identity element of the group.
- **Inverse element:** For each a in G, there exists an element b in G such that $ab = e$ and $ba = e$, where e is the identity element. For each a, the element b is unique, called the inverse of a, denoted a^{-1}.

Question 2. Let $\mathbb{R}$ be the set of real numbers with the operation of addition. Show that $(\mathbb{R}, +)$ is a group.

A group G with the property that $a \circ b = b \circ a$ for all $a, b \in G$ is called abelian or commutative. Groups not satisfying this property are said to be nonabelian or noncommutative. Notice that the set of real numbers under addition have the additional property that $a + b = b + a$ and therefore $(\mathbb{R}, +)$ forms an abelian group. Several other notations are commonly used for groups whose elements are not numbers. For a group whose elements are functions, the operation is often function composition $f \circ g$; then the identity may be denoted id.

Answer :

A1 :

1. **Closure:** The closure property states that for any $x, y \in \Sigma^*$, the concatenation xoy must also belong to Σ^*. Since Σ^* contains all possible strings over the alphabet Σ, the concatenation of any two strings in Σ^* will also result in a string in Σ^*. Therefore, (Σ^*, o, ϵ) is closed under the concatenation operation.
2. **Associativity:** The associativity property states that for any $x, y, z \in \Sigma^*$, the expression $(xoy)oz$ must be equal to $xo(yoz)$. This property holds because the concatenation of strings is inherently associative. When you concatenate three strings, the order in which you group them doesn't affect the final result.
3. **Identity Element:** The identity element is an element $e \in \Sigma^*$ such that for any $x \in \Sigma^*$, $xoe = eox = x$. In this case, the identity element is the empty string ϵ because for any string x, $xo\epsilon = \epsilon ox = x$.

Since (Σ^*, o, ϵ) satisfies all three monoid axioms (closure, associativity, and identity element), it is indeed a monoid.

A2 :

1. **Closure:** The operation of addition on real numbers is closed because if you add two real numbers, the result is also a real number. In other words, for any $a, b \in \mathbb{R}$, $a + b \in \mathbb{R}$.
2. **Associativity:** Addition is an associative operation, which means that for any $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$. Associativity holds for addition, so this axiom is satisfied.
3. **Identity Element** The identity element for addition in the set of real numbers is 0. For any $a \in \mathbb{R}$, $a + 0 = 0 + a = a$. Thus, the identity element is 0.

Since $(\mathbb{R}, +)$ satisfies all four group axioms, it is indeed a group.

20 * (Russell's paradox) In mathematical logic

Answer :

Russell's paradox is a set-theoretical paradox formulated by Bertrand Russell in 1901. The paradox revolves around a set that contains all sets that do not contain themselves. This set can be represented as $R = \{x \mid x \notin x\}$, which includes all sets that satisfy the condition of "not being an element of themselves."

First, let's assume that R is an element of itself, i.e., $R \in R$. According to the definition of the set, R satisfies the condition of "not being an element of itself," thereby contradicting the assumption $R \in R$.

Next, let's assume that R is not an element of itself, i.e., $R \notin R$. According to the definition of the set, R satisfies the condition of "not being an element of itself," thereby fulfilling the assumption $R \notin R$.

However, both assumptions lead to a paradox. If $R \in R$, then R satisfies the condition $R \notin R$, and if $R \notin R$, then R satisfies the condition $R \in R$. This is the core contradiction of Russell's paradox.

Russell's paradox had a profound impact on set theory. It revealed issues of self-reference and paradoxical nature, forcing mathematicians to reexamine the foundations of set theory and revise the axiomatic systems of set theory. This led to further research and development in set theory, aiming to ensure its consistency and reliability. Russell's paradox also sparked investigations into mathematical logic and set theory, driving advancements in the foundations of mathematics.

21 * Often called the language of the universe, mathematics is fundamental to our understanding of the world.

Answer :

22 Given an alphabet Σ, a language is a subset of Σ^*. Two languages L_1 and L_2 are said to be *nonconflicting* if

$\overline{L_1 \cap L_2} = \overline{L_1} \cap \overline{L_2}$

where $\overline{L_i}(i = 1, 2)$ is the prefix-closure of L_i. Give an example of two conflicting languages and an example of two non-conflicting languages. One can use TCT to verify the correctness of her/his results.

> true/false = nonconflict(DES1,DES2) tests whether DES1, DES2 are nonconflicting, namely whether all reachable states of the product DES are coreachable. Not for use with vocalized DES. Note that by doing the product of two DESs, only shared events are executed if their alphabets are not the same.

Answer :

Conflicting Languages:

- Language L_1: 0, 00, 000, ... (The set of all strings consisting of '0' with different lengths, including the empty string ϵ).
- Language L_2: 1, 11, 111, ... (The set of all strings consisting of '1' with different lengths, including the empty string ϵ).

In this case, the prefix-closure of L_1 is L_1, and the prefix-closure of L_2 is L_2. The intersection of their complements ($\overline{L_1} \cap \overline{L_2}$) is still L_1 and L_2, respectively. However, the intersection of the original languages ($\overline{L_1 \cap L_2}$) is the empty set (ϕ), indicating that they are conflicting languages. There are no strings that belong to both L_1 and L_2 in their original forms.

Non-Conflicting Languages:

- Language A: 0, 01, 001, 0001, ... (The set of strings that start with '0' and can have any number of additional '0's or '1's).
- Language B: 1, 10, 110, 1110, ... (The set of strings that start with '1' and can have any number of additional '0's or '1's).

In this case, the prefix-closure of A is A, and the prefix-closure of B is B. The intersection of their complements ($\overline{A} \cap \overline{B}$) is still A and B, respectively. The intersection of the original languages ($\overline{A \cap B}$) is also non-empty and contains strings like "0" and "1" that belong to both A and B. Therefore, A and B are non-conflicting languages.

To verify these results using TCT (Theory of Computation Tools), construct deterministic finite automata (DFAs) for the languages and then compare the intersections to determine whether they are conflicting or non-conflicting.

23 Given an alphabet Σ, a language $L \subseteq \Sigma^*$ is said to be prefix-closed (closed for simplicity) if $L = \overline{L}$. A language $L \subseteq K$ is said to be closed with respect to K, or simply K-closed if $L = \overline{L} \cap K$.

(a) Show that if two languages L_1 and L_2 are K-closed, then $L_1 \cap L_2$ is K-closed.

(b) Show that if $L = \overline{L}$ and define $L' = L \cap K$, then L' is K-closed.

(c) Propose a few examples of languages that are closed or K-closed given a language K.

Answer :

(a) :

$L_1 \cap L_2$ **is Prefix-Closed Within Itself:**

Since L_1 and L_2 are both K-closed, they are individually prefix-closed within themselves. This means that for any string in L_1 or L_2, it does not have any proper prefixes within L_1 or L_2.

Now, consider the intersection $L_1 \cap L_2$. For any string $\omega \in L_1 \cap L_2$, it means that ω is both in L_1 and L_2. Therefore, it follows that ω does not have any proper prefixes within L_1 (because L_1 is prefix-closed), and ω does not have any proper prefixes within L_2 (because L_2 is prefix-closed). As a result, ω does not have any proper prefixes within $L_1 \cap L_2$.

This demonstrates that $L_1 \cap L_2$ is prefix-closed within itself.

$L_1 \cap L_2 \subset K$**:**

Because L_1 and L_2 are both K-closed, it means that they are both subsets of K. That is, for any string in L_1 or L_2, it is also a member of K.

Now, let's consider the intersection $L_1 \cap L_2$. For any string $\sigma \in L_1 \cap L_2$, it means that ω is both in L_1 and L_2. Since L_1 and L_2 are both subsets of K, it follows that σ is a member of K as well, as it satisfies the condition of being in both L_1 and L_2.

This demonstrates that $L_1 \cap L_2 \subset K$.

Therefore, we have shown that $L_1 \cap L_2$ is both prefix-closed within itself and a subset of K, which means that it is K-closed, as required.

(b) :

we need to demonstrate that L' satisfies the properties of being prefix-closed within itself and being a subset of K.

1. L' is Prefix-Closed Within Itself:

   Given that $L = \overline{L}$, it means that L is a prefix-closed language within itself. For any string $\omega \in L$, it does not have any proper prefixes within L.

   Now, consider the language L'. For any string $\omega \in L'$, it means that ω is both in L (which is prefix-closed) and in K. Since $\omega \in L$, it does not have any proper prefixes within L. Additionally, because $\omega \in K$, it follows that ω is a member of K.

   Therefore, ω does not have any proper prefixes within L' (since it doesn't have any within L), and ω is a member of K.

   This demonstrates that L' is prefix-closed within itself.

2. L' is a Subset of K:

   Given that $L' = L \cap K$, it implies that L' is the intersection of L and K. Therefore, for any string $\omega \in L'$, it means that ω is both in L and in K.

   Since $L = \overline{L}$, it follows that for any string in L (including those in L'), they do not have any proper prefixes within L. Additionally, because $\omega \in K$, it follows that ω is a member of K.

   This demonstrates that L' is a subset of K.

   Therefore, we have shown that L' is both prefix-closed within itself and a subset of K, which means that it is K-closed, as required.

(c) :

Closed Languages ($L = \overline{L}$):

1. Language $L_1 : \{\epsilon\}$ (the language containing only the empty string)

   L_1 is closed because it is equal to its own complement. There are no proper prefixes of ϵ, so it is prefix-closed.

2. Language $L_2 : \{0, 1, 00, 11, \ldots\}$ (the set of all strings consisting of '0' and '1', including the empty string ϵ)

   L_2 is closed because it contains all possible strings of '0' and '1', and there are no proper prefixes within itself.

K-Closed Languages ($L = \overline{L} \cap K$):

1. Language $A : \{0, 00, 000, \ldots\}$ (the set of all strings consisting of '0' with different lengths, including the empty string ϵ)

   If $K = \{0\}$, then A is K-closed because it is the intersection of its own complement and K. A consists of strings without proper prefixes, and it is a subset of K.

2. Language $B : \{1, 11, 111, \ldots\}$ (the set of all strings consisting of '1' with different lengths, including the empty string ϵ)

   If $K = \{1\}$, then B is K-closed because it is the intersection of its own complement and K. B consists of strings without proper prefixes, and it is a subset of K.

3. Language $C : \{\epsilon, 00, 11, 0000, 1111, \ldots\}$ (the set of all strings consisting of repeated '0's or '1's, including the empty string ϵ)

   If $K = \{\epsilon, 0, 1\}$, then C is K-closed because it is the intersection of its own complement and K. C consists of strings without proper prefixes, and it is a subset of K.

4. Language $D : \{ab, aab, aaab, \ldots\}$ (the set of strings with 'a's followed by one or more 'b's)

   If $K = \{ab, aab, \ldots\}$, then D is K-closed because it is the intersection of its own complement and K. D consists of strings without proper prefixes, and it is a subset of K.

24 Δ One refers to a review article on the history of supervisory control theory (SCT) of DES if she/he is interested in the development of DES modeling,

analysis and control, see [W. M. Wonham, K. Cai, and K. Rudie, Supervisory control of discrete event systems: A brief history, Annual Annual Reviews in Control, vol. 45, 2018, Pages 250-256]. A similar version can be found in `https://www.control.utoronto.ca/~wonham/Wonham_SCDES_history.pdf`

Answer :

According to the provided document, it is a brief history article on "Supervisory Control of Discrete-Event Systems" from 1980 to 2015. The article summarizes the development of this field during that period, noting the transition from centralized or "monolithic" control to more structured architectures, as well as the shift from "naive" to symbolic computation. The authors acknowledge that, like any history, some important contributions may have been overlooked or not fully addressed.

The document starts by mentioning the background and early motivation of supervisory control of discrete-event systems around 1980. It highlights the distinction between discrete-event systems and continuous systems controlled by differential equations. Discrete-event systems are characterized by being discrete in time and state space, driven by instantaneous events, and non-deterministic in making state-transitional choices.

The article then discusses the development of language controllability and monolithic supervisory control from 1981 to 1987. It describes how discrete-event systems control theory emerged, where the plant and control specification were modeled as finite-state machines. The control technology involved partitioning the language alphabet into controllable and uncontrollable events, with the controllable events being subject to disablement by a supervisor. The problem of supervisory control synthesis was formalized as the design of a finite-state supervisor that disables a suitable subset of controllable events to ensure that the controlled behavior satisfies the control specification.

The concept of qualitative optimality was introduced to ensure that the controlled behavior is as rich as possible while still satisfying the specification constraint. The theory also introduced the concept of controllable language and the idea that the controllable sublanguages of a given specification language have a unique maximal element. The solution to the problem of optimal control is the top element of this semilattice of controllable sublanguages.

In summary, the article provides an overview of the history of supervisory control of discrete-event systems, highlighting important developments and trends from 1980 to 2015.

25 * (Petri nets and discrete event systems) Petri nets serve as an important yet powerful alternative to automata for the modeling and control of untimed DES.

Answer :

optional

26 ** Conventionally, people think of models as either toys or simple copies of reality.

Answer :

optional

27 A computer system operates with two parallel processors P1 and P2. The total capacity (queue and server included) of P1 is $K_1 = 1$, and that of P2 is $K_2 = 2$. The system receives two types of jobs, labeled J_1 and J_2. Jobs of type J_1 must be processed at P1, and jobs of type J_2 must be processed at P2. When a job is processed, it leaves the system. If a job finds a full queue upon arrival, then the job is simply rejected. Build an automaton model of this system.

Four events are identified:
a_i: arrival of J_i
d_i: departure of J_i.
A state is of the form (n_1, n_2) where n_i is the number of jobs in (queue and server) in processor P_i.
Note that the model has six states totally.

Answer :

States:

- State (0, 0): Initial state. No jobs are in the system.
- State (1, 0): A job of type J_1 is in the queue for P1.
- State (2, 0): Two jobs of type J1 are in the queue for P1 (queue full, no room for J_2).
- State (0, 1): A job of type J_2 is in the queue for P2.
- State (0, 2): Two jobs of type J_2 are in the queue for P2 (queue full, no room for J_1).
- State (1, 1): A job of type J_1 is in the queue for P1, and a job of type J_2 is in the queue for P2 (both queues occupied).

Transitions:

1. From State (0, 0):
   - On arrival of a job of type J_1, transition to State (1, 0).
   - On arrival of a job of type J_2, transition to State (0, 1).
2. From State (1, 0):
   - On arrival of another job of type J_1, transition to State (2, 0) (queue for P1 is full).
   - On arrival of a job of type J_2, transition to State (1, 1) (J_2 joins P2's queue).
   - On departure of the J_1 job from P1, transition back to State (0, 0).
3. From State (2, 0):
   - On arrival of a job of type J_1, stay in State (2, 0) (queue is full, job rejected).
   - On arrival of a job of type J_2, stay in State (2, 0) (queue is full, job rejected).
   - On departure of the J_1 job from P1, transition to State (0, 0) (queue for P1 is free).
4. From State (0, 1):
   - On arrival of a job of type J_1, transition to State (1, 1) (J_1 joins P1's queue).
   - On arrival of another job of type J_2, transition to State (0, 2) (queue for P2 is full).
   - On departure of the J_2 job from P2, transition back to State (0, 0).
5. From State (0, 2):
   - On arrival of a job of type J_1, stay in State (0, 2) (queue is full, job rejected).
   - On arrival of a job of type J_2, stay in State (0, 2) (queue is full, job rejected).

- On departure of the J_2 job from P2, transition to State (0, 1) (queue for P2 is free).

6. From State (1, 1):
   - On arrival of another job of type J_1, stay in State (1, 1) (both queues are full, job rejected).
   - On arrival of another job of type J_2, stay in State (1, 1) (both queues are full, job rejected).
   - On departure of the J_1 job from P1, transition to State (0, 1) (queue for P1 is free).
   - On departure of the J_2 job from P2, transition to State (1, 0) (queue for P2 is free).

28 A workcell consists of two machines M1 and M2 and an automated guided vehicle AGV, along with two auxiliary devices: input buffer and output buffer whose capacity is assumed to be large enough.

Answer :

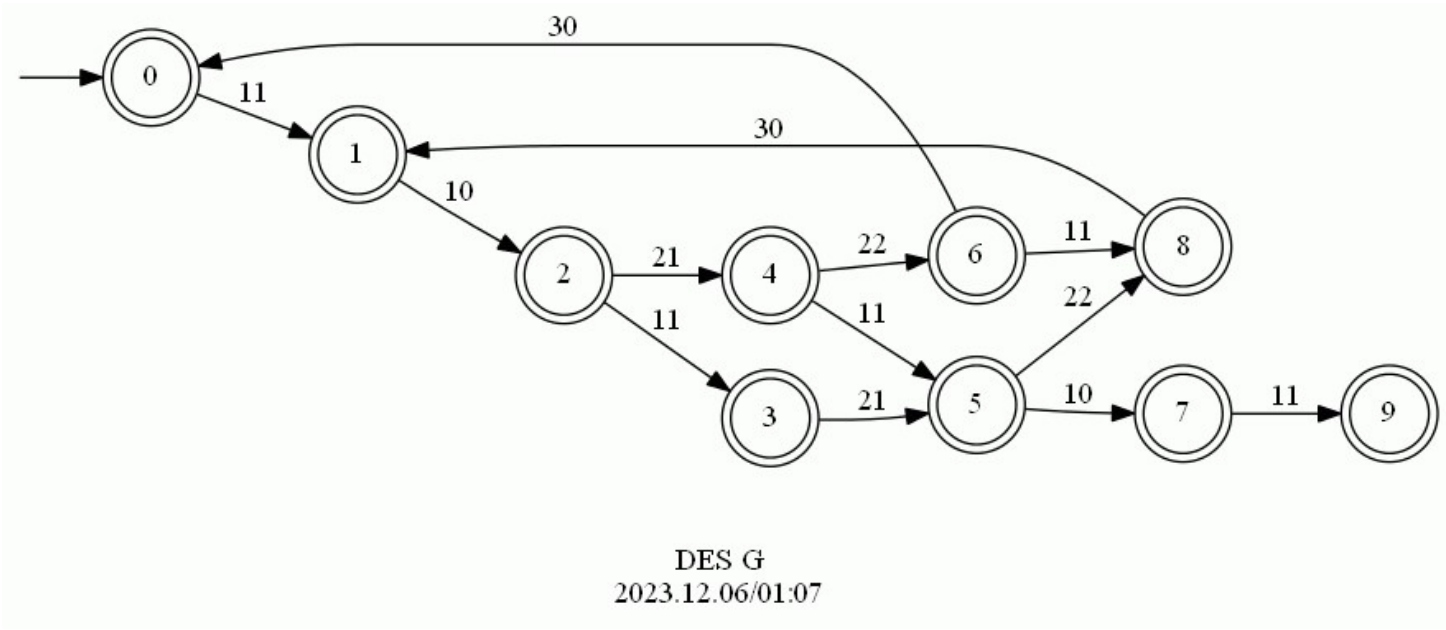

Figure 1: G

1. Find G

   As shown in Figure 1.

2. Check G is blocking or nonblocking (that can be done by using TCT)

   To check if G is blocking or nonblocking, we can use the TCT (Transition Closure Table) method. The TCT method involves iteratively computing the reachable states from the initial state and checking if there are any deadlock states (states from which no further transitions are possible).

3. If G is not non-blocking, analyse the blocking states and the event sequences leading to the blocking states from the initial state

   If G is found to be blocking, we can analyze the blocking states and the event sequences leading to them from the initial state. Blocking states are states from which no further progress can be made, i.e., no transitions are enabled.

4. Propose a supervisory control strategy such that the controlled system is non-blocking (one could use TCT to verify the proposed non-blocking strategy).

   To propose a supervisory control strategy that ensures non-blocking behavior, we can use the TCT method to verify the proposed strategy. The goal is to design a supervisor that allows the system to reach only non-blocking states and avoids deadlock or blocking situations.

29 Propose the Petri net model for the system in Question 28.

Answer :

30 Given $L, L_1, L_2, L_3 \subseteq \Sigma^*$, show

$$L \subseteq \overline{L},$$
$$\overline{L_1 \cap L_2} \subseteq \overline{L_1} \cap \overline{L_2},$$
$$L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3, and.$$
$$L_1(L_2 \cap L_3) = L_1L_2 \cap L_1L_3.$$

Answer :

- $L \subseteq \overline{L}$

  To show that a language L is a subset of its complement, you want to prove that for every string x in L, it is also in $\overline{L}$, which means that $L \subseteq \overline{L}$.

  Here's the formal proof:

  Let x be an arbitrary string in L. This means that x is an element of L. Since x is in L, it is also not in $\overline{L}$, by definition. Therefore, x is in L and not in $\overline{L}$.

  Because x was an arbitrary string chosen from L, this proof holds for all strings in L. Therefore, we can conclude that for every string x in L, x is also in $\overline{L}$, which means $L \subseteq \overline{L}$.

  In other words, the entire language L is a subset of its own complement $\overline{L}$.

- $\overline{L_1 \cap L_2} \subseteq \overline{L_1} \cap \overline{L_2}$

  To show that $\overline{L_1 \cap L_2} \subseteq \overline{L_1} \cap \overline{L_2}$, we need to prove that if a string is in the complement of the intersection of two languages L_1 and L_2, then it is also in the intersection of the complements of these languages.

  Let's use set notation to represent this:

  $\overline{L_1 \cap L_2}$ represents the complement of the intersection of L_1 and L_2.

  $\overline{L_1} \cap \overline{L_2}$ represents the intersection of the complements of L_1 and L_2.

  We want to prove that for any string x:

  If $x \in \overline{L_1 \cap L_2}$, then $x \in \overline{L_1} \cap \overline{L_2}$.

  Here's the proof:

  Suppose $x \in \overline{L_1 \cap L_2}$. This means that x is not in the intersection of L_1 and L_2. In other words, $x \notin (L_1 \cap L_2)$.

  Now, we can use De Morgan's Law, which states that the complement of an intersection is equal to the union of complements:

  $\overline{L_1 \cap L_2} = \overline{L_1} \cup \overline{L_2}$

  So, we have $x \in (\overline{L_1} \cup \overline{L_2})$. This means that x is in either the complement of L_1 or the complement of L_2, or both.

  Therefore, $x \in \overline{L_1}$ and $x \in \overline{L_2}$.

  This is precisely what is represented by $x \in \overline{L_1} \cap \overline{L_2}$, which is the intersection of the complements of L_1 and L_2.

  So, we have shown that if $x \in \overline{L_1 \cap L_2}$, then $x \in \overline{L_1} \cap \overline{L_2}$, which proves the inclusion $\overline{L_1 \cap L_2} \subseteq \overline{L_1} \cap \overline{L_2}$.

- $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$

  To prove that $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$, we need to show that every string in the left-hand side (LHS) language is also in the right-hand side (RHS) language, and vice versa.

  Let's break this proof into two parts:

  Part 1: Proving $L_1(L_2 \cup L_3) \subseteq L_1L_2 \cup L_1L_3$:

  Let x be a string in $L_1(L_2 \cup L_3)$. This means that x is of the form $x = yz$, where $y \in L_1$ and $z \in (L_2 \cup L_3)$. Since $z \in (L_2 \cup L_3)$, it means that z can be either in L_2 or L_3.

  1. If $z \in L_2$, then yz is in L_1L_2, and therefore, x is in $L_1L_2 \cup L_1L_3$.

2. If $z \in L_3$, then yz is in L_1L_3, and therefore, x is in $L_1L_2 \cup L_1L_3$.

In both cases, x is in $L_1L_2 \cup L_1L_3$. Therefore, we have shown that $L_1(L_2 \cup L_3) \subseteq L_1L_2 \cup L_1L_3$.

Part 2: Proving $L_1(L_2 \cup L_3) \supseteq L_1L_2 \cup L_1L_3$:

Let x be a string in $L_1L_2 \cup L_1L_3$. This means that x is either in L_1L_2 or L_1L_3.

1. If x is in L_1L_2, it means $x = yz$, where $y \in L_1$ and $z \in L_2$. Since $z \in L_2$, we can say that z is in $(L_2 \cup L_3)$, and therefore, x is in $L_1(L_2 \cup L_3)$.
2. If x is in L_1L_3, it means $x = yz$, where $y \in L_1$ and $z \in L_3$. Similar to the first case, since $z \in L_3$, we can say that z is in $(L_2 \cup L_3)$, and therefore, x is in $L_1(L_2 \cup L_3)$.

In both cases, x is in $L_1(L_2 \cup L_3)$. Therefore, we have shown that $L_1(L_2 \cup L_3) \supseteq L_1L_2 \cup L_1L_3$.

Combining both parts, we have proven that $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$.

- $L_1(L_2 \cap L_3) = L_1L_2 \cap L_1L_3$

  To prove that $L_1(L_2 \cap L_3) = L_1L_2 \cap L_1L_3$, we need to show that every string in the left-hand side (LHS) language is also in the right-hand side (RHS) language, and vice versa.

  Let's break this proof into two parts:

  Part 1: Proving $L_1(L_2 \cap L_3) \subseteq L_1L_2 \cap L_1L_3$:

  Let x be a string in $L_1(L_2 \cap L_3)$. This means that x is of the form $x = yz$, where $y \in L_1$ and $z \in (L_2 \cap L_3)$. Since $z \in (L_2 \cap L_3)$, it means that z is in both L_2 and L_3.

  1. Since $y \in L_1$ and $z \in L_2$, yz is in L_1L_2, and therefore, x is in $L_1L_2 \cap L_1L_3$.
  2. Since $y \in L_1$ and $z \in L_3$, yz is in L_1L_3, and therefore, x is in $L_1L_2 \cap L_1L_3$.

  In both cases, x is in $L_1L_2 \cap L_1L_3$. Therefore, we have shown that $L_1(L_2 \cap L_3) \subseteq L_1L_2 \cap L_1L_3$.

  Part 2: Proving $L_1(L_2 \cap L_3) \supseteq L_1L_2 \cap L_1L_3$:

  Let x be a string in $L_1L_2 \cap L_1L_3$. This means that x is in both L_1L_2 and L_1L_3.

  1. If x is in L_1L_2, it means $x = yz$, where $y \in L_1$ and $z \in L_2$. Since $z \in L_2$, it follows that z is in $L_2 \cap L_3$, and therefore, x is in $L_1(L_2 \cap L_3)$.
  2. If x is in L_1L_3, it means $x = yz$, where $y \in L_1$ and $z \in L_3$. Similar to the first case, z is in $L_2 \cap L_3$, and therefore, x is in $L_1(L_2 \cap L_3)$.

  In both cases, x is in $L_1(L_2 \cap L_3)$. Therefore, we have shown that $L_1(L_2 \cap L_3) \supseteq L_1L_2 \cap L_1L_3$.

  Combining both parts, we have proven that $L_1(L_2 \cap L_3) = L_1L_2 \cap L_1L_3$.

31 Let G be a generator with the alphabet Σ and $K \subseteq \Sigma^*$ be a language. Show $\overline{K} \subseteq L(G)$ if $K \subseteq L(G)$: [hint: L(G) is prefix-closed].

Answer : To prove that the complement of language $\overline{K} \subseteq L(G)$ when $K \subseteq of L(G)$, given that L(G) is prefix-closed, we can use the property of prefix-closed languages.

Proof:

Suppose $K \subseteq L(G)$. This means that for every string x in K, x is also in L(G) because $K \subseteq L(G)$.

Since L(G) is prefix-closed, we know that if a string x is in L(G), all of its prefixes are also in L(G).

Now, let's consider the complement of K, which is $\overline{K}$. For any string y in $\overline{K}$, it means that y is not in K (because $\overline{K}$ is the set of all strings not in K).

Since $K \subseteq L(G)$, if y is not in K, it is also not in L(G). This is because L(G) contains K, and if a string is not in K, it's not in L(G) either.

Therefore, for any string y in $\overline{K}$, it is not in K, and it is also not in L(G).

This implies that every string in $\overline{K}$ is also not in L(G), which is equivalent to saying that $\overline{K} \subseteq L(G)$.

In conclusion, if $K \subseteq L(G)$ and L(G) is prefix-closed, then the complement of K, $\overline{K} \subseteq L(G)$.

32 Given a generator G with $\Sigma = \{a, b, c\}$ as shown below, assume that b is not observable. Find P (G).

Answer : Determine the probability $P(G)$ for the given generator G with $\Sigma = \{a, b, c\}$, where b is not observable.

To find $P(G)$, we need to analyze the information available in the documents. Unfortunately, the documents do not directly provide the probability $P(G)$. However, we can make some observations based on the information given.

K is not observable with respect to G and P. This implies that the events in K, which includes b, cannot be directly observed in G.

$\Sigma = \{a, b, c, d, e, f, g\}$. Although it is not directly related to the given generator G, it gives us some insight into the control and observability aspects of discrete event systems.

Based on the available information, we can conclude that the probability $P(G)$ cannot be determined solely from the given documents. We would need additional information or specifications about the behavior and transitions of the generator G to calculate the probability.

33 Show the properties of projection.

1. If $A \subseteq B$, $PA \subseteq PB$ and $P^{-1}A \subseteq P^{-1}B$.
2. $P[P^{-1}(L)] = L$; $L \subseteq P^{-1}[P(L)]$.
3. $P(A \cup B) = PA \cup PB$.
4. $P^{-1}(A \cup B) = P^{-1}(A) \cup P^{-1}(B)$; $P^{-1}(A \cap B) = P^{-1}(A) \cap P^{-1}(B)$.
5. $P(AB) = P(A)P(B)$; $P^{-1}(AB) = P^{-1}(A)P^{-1}(B)$.

Answer :

Chapter 4. page:89

1. If $A \subseteq B$, then $PA \subseteq PB$ and $P^{-1}A \subseteq P^{-1}B$.

   Proof:

   Let $s \in PA$. There necessarily exist $t \in \Sigma^*$ such that $t \in A$ and $Pt = s$. By $A \subseteq B$, $t \in B$. We have $Pt = s \in PB$

   Let $s \in P^{-1}A$. Then there exist $t \in A$ such that $Ps = t$. By $A \subseteq B$, $Ps \in B$ and $s \in P^{-1}B$

   In the proof above, from $Ps \in B$, we cannot directly infer $P^{-1}[Ps] \subseteq P^{-1}B$ and cannot derive $s \in P^{-1}B$ by $s \in P^{-1}[Ps]$.

   Portray $Ps \in B$ naturally means $s \in P^{-1}B$

2. $P[P^{-1}(L)] = L$; $L \subseteq P^{-1}[P(L)]$.

   (a) $P[P^{-1}(L)] = L$

   Proof:

   To show $P[P^{-1}(L)] \subseteq L$, we need to prove $P[P^{-1}(L)] \subseteq L$ and $L \subseteq P[P^{-1}(L)]$.

   - let $s \in P[P^{-1}(L)]$, there necessarily exists $t \in \Sigma^*$ such that $t \in P^{-1}(L)$ and $Pt = s$. By $t \in P[P^{-1}(L)]$, $Pt \in L$(Note that $P^{-1}(L) = \{s\prime \in \Sigma^* | (\exists s \in L) Ps\prime = s\}$). We have $Pt = s \in L$ and thus $P[P^{-1}(L)] \subseteq L$
   - To show $L \subseteq P[P^{-1}(L)]$, let $s \in L$. $P^{-1}\{s\} \subseteq P^{-1}(L)$. $P[P^{-1}\{s\}] \subseteq P[P^{-1}(L)]]$ (by Property 1). By $s \in P[P^{-1}\{s\}]$, $s \in P[P^{-1}(L)]$ then $L \subseteq P[P^{-1}(L)]$ holds.

   (b) $L \subseteq P^{-1}[P(L)]$

   Proof:

   let $s \in L$.

   $\{s\} \subseteq L \Rightarrow P\{s\} \subseteq PL \Rightarrow P^{-1}[P\{s\}] \subseteq P^{-1}[P(L)]$.

   By $s \in P^{-1}[P\{s\}]$, we have $s \in P^{-1}[P(L)]$.

   We conclude $L \subseteq P^{-1}[P(L)]$.

3. $P(A \cup B) = P(A) \cup P(B)$.

   Proof:

   ($\subseteq$) Let $s \in P(A \cup B)$. There necessarily exists $t \in \Sigma^*$ such that $t \in A \cup B$ and $Pt = s$. We have three cases:

(i) $t \in A$ and $t \notin B$. Then $Pt \in PA$, i.e., $s \in PA$. Thus, $s \in PA \cup PB$

(ii) $t \in B$ and $t \notin A$. Then $Pt \in PB$, i.e., $s \in PB$. Thus, $s \in PA \cup PB$

(iii) $t \in A$ and $t \in B$. Then $Pt \in PA$ and $Pt \in PB$. Thus, $s \in PA \cup PB$

Finally, we have $P(A \cup B) \subseteq P(A) \cup P(B)$.

($\supseteq$) Let $s \in P(A) \cup P(B)$. Then two cases are considered.

(i) $s \in P(A)$ and $s \notin P(B)$(or $[s \in P(B) \& s \notin P(A)]$). There exists $t \in \Sigma^*$ such that $t \in A$ and $Pt = s$. Then, we have $t \in A \cup B$ and $Pt = s \in P(A \cup B)$.

(ii) $s \in P(A)$ and $s \in P(B)$. There exists $t_1 \in \Sigma^*$ and $t_2 \in \Sigma^*$ such that $t_1 \in A$, $t_2 \in B$ and $Pt_1 = Pt_2 = s$. $t_1 \in A \cup B$, $Pt_1 = s \in P(A \cup B)$. Thus, $PA \cup PB \subseteq P(A \cup B)$.

4. $P^{-1}(A \cup B) = P^{-1}(A) \cup P^{-1}(B)$; $P^{-1}(A \cap B) = P^{-1}(A) \cap P^{-1}(B)$.

(a) $P^{-1}(A \cup B) = P^{-1}(A) \cup P^{-1}(B)$.

Proof:

($\subseteq$) $P^{-1}(A \cup B) \subseteq P^{-1}(A) \cup P^{-1}(B)$.

Let $s \in P^{-1}(A \cup B)$. $(\exists t \in \Sigma^*) t \in A \cup B$ such that $Ps = t$.

(i) $Ps \in A$, $Ps \notin B$
$P^{-1}(Ps) \subseteq P^{-1}(A)$. $s \in P^{-1}(Ps)$, $s \in P^{-1}(A)$
$s \in P^{-1}(A) \Rightarrow s \in P^{-1}(A) \cup P^{-1}(B)$.

(ii) $Ps \notin A$, $Ps \in B$
$P^{-1}(\{Ps\}) \subseteq P^{-1}(B)$.
$s \in P^{-1}(Ps)$, $s \in P^{-1}(B) \Rightarrow s \in P^{-1}(B) \cup P^{-1}(A)$

(iii) $Ps \in A$, $Ps \in B$
$P^{-1}(\{Ps\}) \subseteq P^{-1}(A)$ and $P^{-1}(Ps) \subseteq P^{-1}(B)$
By $s \in P^{-1}(\{Ps\})$, then
$s \in P^{-1}(A)$, $s \in P^{-1}(B)$, $s \in P^{-1}(A) \cup P^{-1}(B)$

($\supseteq$) Show $P^{-1}(A) \cup P^{-1}(B) \supseteq P^{-1}(A \cup B)$.

Let $s \in P^{-1}(A) \cup P^{-1}(B)$. Three cases:

(i) $s \in P^{-1}(A)$, $s \notin P^{-1}(B)$
$Ps \in A \Rightarrow Ps \in A \cup B$
$P^{-1}(\{Ps\}) \subseteq P^{-1}(A \cup B)$
By $s \in P^{-1}(\{Ps\})$, $s \in P^{-1}(A \cup B)$.

(ii) $s \in P^{-1}(B)$, $s \notin P^{-1}(A)$ (similar to (i))

(iii) $s \in P^{-1}(A)$ and $s \in P^{-1}(B)$
$Ps \in A$, $Ps \in B \Rightarrow Ps \in A \cup B$
$P^{-1}(\{Ps\}) \subseteq P^{-1}(A \cup B)$
$s \in P^{-1}(\{Ps\}) \Rightarrow s \in P^{-1}(A \cup B)$

Finally, we have
$P^{-1}(A \cup B) = P^{-1}(A) \cup P^{-1}(B)$

(b) $P^{-1}(A \cap B) = P^{-1}(A) \cap P^{-1}(B)$.

Proof:

($\subseteq$) Let $s \in P^{-1}(A \cap B)$.

$(\exists t \in \Sigma^*) t \in A \cap B$ and $Ps = t$

$t \in A$ and $t \in B$

Since $s \in P^{-1}(\{Ps\}) = P^{-1}\{t\}$, $s \in P^{-1}(A)$ and $s \in P^{-1}(B)$

$s \in P^{-1}(A) \cap P^{-1}(B)$

($\supseteq$) Let $s \in P^{-1}(A) \cap P^{-1}(B)$, i.e., $s \in P^{-1}(A)$ and $s \in P^{-1}(B)$

$Ps \in A$ and $Ps \in B$ $Ps \in (A \cap B)$

$P^{-1}(\{Ps\}) \subseteq P^{-1}(A \cap B)$

By $s \in P^{-1}(\{Ps\})$, $s \in P^{-1}(A \cap B)$

$P^{-1}(A) \cap P^{-1}(B) \subseteq P^{-1}(A \cap B)$.

5. $P(AB) = P(A)P(B)$; $P^{-1}(AB) = P^{-1}(A)P^{-1}(B)$.

(a) $P(AB) = P(A)P(B)$.
Proof:
($\subseteq$) Let $s \in P(AB)$. $(\exists t \in \Sigma^*)t \in AB$ and $Ps = t$. Since
$AB = \{s_1 s_2 \mid s_1 \in A, s_2 \in B\}$,
Let $t = t_1 t_2$ with $t_1 \in A$ and $t_2 \in B$.
$Pt = Pt_1 \cdot Pt_2 \in P(A)P(B)$
$s \in P(A)P(B)$
($\supseteq$) Let $s \in P(A)P(B)$ with $s = s_1 s_2$.
$P(A)P(B) = \{s_1 s_2 \mid s_1 \in P(A), s_2 \in P(B)\}$
$s_1 \in P(A) \Rightarrow \exists t_1 \in A Pt_1 = t_1$
$s_2 \in P(B) \Rightarrow \exists t_2 \in B Pt_2 = t_2$
By $t_1 t_2 \in AB$, $P(t_1 t_2) = P(t_1)P(t_2) = s_1 s_2 = s \in P(AB)$.

(b) $P^{-1}(AB) = P^{-1}(A)P^{-1}(B)$.
Proof:
($\subseteq$) Let $s \in P^{-1}(AB)$. $Ps \in AB$
$(\exists s_1 s_2 \in \Sigma^*) Ps_1 \in A$, $Ps_2 \in B$, $s = s_1 s_2$
$p^{-1}(Ps_1) \subseteq P^{-1}(A)$, $p^{-1}(Ps_2) \subseteq P^{-1}(B)$
Since $s_1 \in P^{-1}(Ps_1)$, $s_2 \in P^{-1}(Ps_2)$
$s_1 s_2 \in P^{-1}(A)P^{-1}(B)$
($\supseteq$) Let $s \in P^{-1}(A)P^{-1}(B)$
$(\exists t_1 t_2 \in \Sigma^*) t_1 \in A$, $t_2 \in B$ $Ps = t_1 t_2$
$t_1 t_2 \in AB$, $P{-}1(t_1 t_2) \subseteq P^{-1}(AB)$. $P^{-1}(Ps) \subseteq P^{-1}(AB)$.
$s \in P^{-1}(Ps) \Rightarrow s \in P^{-1}(AB)$.

Proof: (to be completed)

34 Given H, K, L, and $\Sigma = \Sigma_c \dot{\cup} \Sigma_u$ such that $H \subseteq K = K \subseteq L = L \subseteq \Sigma^*$, suppose that H is controllable with respect to K and Σ_u and K is controllable with respect to L and Σ_u. Show that H is controllable with respect to L and Σ_u (check whether $L = \overline{L}$ is a necessity for the controllability of H with respect to L and Σ_u).

Answer :

To prove that H is controllable with respect to L and Σ_u, we need to show that for any two states $h_1, h_2 \in H$ and any string $w \in \Sigma_u^*$, there exists a control sequence $u \in \Sigma_u^*$ such that the system starting from h_1 and applying control sequence u reaches state h_2 and the output sequence is in L.

Given that H is controllable with respect to K and Σ_u, we know that for any two states $h_1, h_2 \in H$ and any string $u \in \Sigma_u^*$, there exists a control sequence $v \in \Sigma_u^*$ such that the system starting from h_1 and applying control sequence v reaches state h_2 and the output sequence is in K.

Similarly, we are given that K is controllable with respect to L and Σ_u, which means that for any two states $k_1, k_2 \in K$ and any string $u \in \Sigma_u^*$, there exists a control sequence $w \in \Sigma_u^*$ such that the system starting from k_1 and applying control sequence w reaches state k_2 and the output sequence is in L.

Now, let's consider two states $h_1, h_2 \in H$ and a string $u \in \Sigma_u^*$. Since H is controllable with respect to K and Σ_u, there exists a control sequence $v \in \Sigma_u^*$ such that the system starting from h_1 and applying control sequence v reaches state h_2 and the output sequence is in K.

Since K is controllable with respect to L and Σ_u, there exists a control sequence $w \in \Sigma_u^*$ such that the system starting from $k_1 = h_1$ (as $h_1 \in H \subseteq K$) and applying control sequence w reaches state $k_2 = h_2$ (as $h_2 \in H \subseteq K$) and the output sequence is in L.

Therefore, we have shown that for any two states $h_1, h_2 \in H$ and any string $u \in \Sigma_u^*$, there exists a control sequence $w \in \Sigma_u^*$ such that the system starting from h_1 and applying control sequence w reaches state h_2 and the output sequence is in L.

In conclusion, H is controllable with respect to L and Σ_u.

Regarding the necessity of $L = \overline{L}$ for the controllability of H with respect to L and Σ_u, it is not a necessity. The controllability of H with respect to L and Σ_u depends on the existence of control sequences that can steer the system from one state to another while generating the desired output sequence. The condition $L = \overline{L}$ is not directly related to this concept.

35 Let MACH as depicted below be a generator with $\Sigma = \{\alpha, \beta, \lambda, \mu\}$, where α and μ are controllable. Suppose that the SPEC is $K = \{\alpha\beta\alpha\beta\}$, i.e., MACH is shut down after two successful production cycles. By intuition, check if there exists a supervisor that can supervise MACH to implement this SPEC. If existing, portray it; otherwise, explain the reason of non-existence. Consider the case that $K = \{\alpha\beta\}$.

Answer :

As Figure 2 shows.

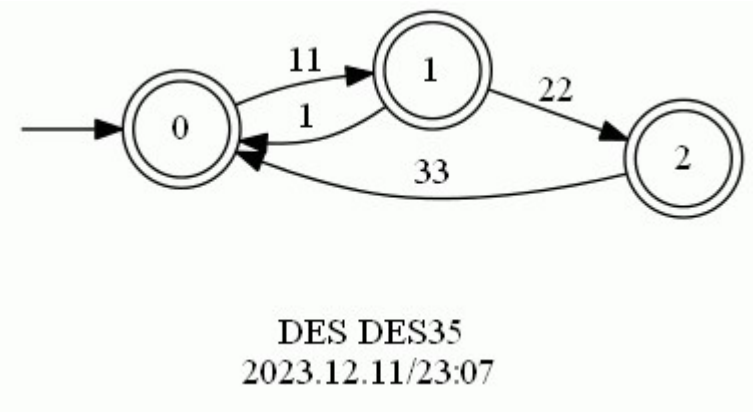

Figure 2: Homework 35

36 Review the notion of equivalence relation and propose 2-3 examples of equivalence relations in our daily life.

Answer :

1. Friendship: Consider a group of friends. We can define an equivalence relation on this group based on friendship. Two individuals are related if they are friends with each other. This relation is reflexive (everyone is a friend of themselves), symmetric (if person A is a friend of person B, then person B is a friend of person A), and transitive (if person A is a friend of person B, and person B is a friend of person C, then person A is a friend of person C).

2. Equality: In mathematics, the relation of equality is an equivalence relation. Two numbers are related if they are equal to each other. This relation is reflexive (every number is equal to itself), symmetric (if a = b, then b = a), and transitive (if a = b and b = c, then a = c).

3. Language: In linguistics, we can define an equivalence relation based on language dialects. Two individuals are related if they speak the same dialect. This relation is reflexive (everyone speaks the dialect they are associated with), symmetric (if person A speaks the same dialect as person B, then person B speaks the same dialect as person A), and transitive (if person A speaks the same dialect as person B, and person B speaks the same dialect as person C, then person A speaks the same dialect as person C).

37 Given a plant G with some control specification

Given a plant G with some control specification, the set of control patterns is $\Gamma = \{\gamma \mid \Sigma_u \subseteq \gamma\}$, i.e., a control pattern γ is usually a super-set of Σ_u. Suppose that V is a supervisory control function that implements the control specification. Given

$s \in L(G), V(s) \in \Gamma$ defines the set of events that are feasible or active after s is generated by G. It implies that the events in $\Sigma - V(s)$ should be disabled upon the occurrence of s.

Let $f(s) = \Sigma - V(s)$. The generated language $L(f/G)$ and the marked language $L_m(f/G)$ of the controlled system under the supervision of f are respectively defined as

1. $\varepsilon \in L(f/G); (\forall s \in \Sigma^*)\,(\forall \sigma \in \Sigma)[s \in L(f/G)]\&[s\sigma \in L(G)]\&[\sigma \notin f(s)] \Rightarrow s\sigma \in L(f/G)$.
2. $L_m(f/G) = L(f/G) \cap L_m(G)$

Answer :

1. Obviously, $L(f/G) \subseteq \overline{L(f/G)}$
2. To show $\overline{L(f/G)} \subseteq L(f/G)$, let $s \in \overline{L(f/G)}$.

Then, $(\exists t \in \Sigma^*)$ st $\in L(f/G)$. By induction, let $t = \varepsilon$ or $t = \sigma \in \Sigma$. Then $s \in L(f/G)$ (by definition of $L(f/G)$). (continued) Suppose that $s \in L(f/G), t = \sigma_1\sigma_2 \cdots \sigma_k$, and $st \in L(f/G)$, where $\sigma_i \in \Sigma, i \in \mathbb{N}_k$.

We will show $s \in L(f/G)$ if $t = \sigma_1\sigma_2 \cdots \sigma_k\sigma_k + 1$ and $st \in L(f/G)$. Then,

$$\sigma_{k+1} \in V\left(s\sigma_1\sigma_2 \cdots \sigma_k\right)$$

and

$$s\sigma_1\sigma_2 \cdots \sigma_k\sigma_{k+1} \in L(G)$$

By $s\sigma_1\sigma_2 \cdots \sigma_k \in L(f/G)$ (by assumption) and $s\sigma_1\sigma_2 \cdots \sigma_k \in L(G)$[since L(G) is closed],

$$\sigma_k \in V\left(s\sigma_1\sigma_2 \cdots \sigma_{k-1}\right)$$

Thus, $s\sigma_1\sigma_2 \cdots \sigma_{k-1} \in L(f/G)$. By induction, we reach $s\sigma_1 \in L(f/G)$, implying that $s \in L(f/G), \sigma_1 \in V(s), s\sigma_1 \in L(G)$. Thus it holds $s \in L(f/G)$.

38 Given $K \subseteq \Sigma^*$, prove that there exists a Σ_u-enabling, non-marking, and non-blocking supervisor such that $L(G||S) = K$ if and only if $\emptyset \neq K = \overline{K} = \overline{L_m(G) \cap K}$ and K is controllable.

39 Let G be a plant and $K_1, K_2 \subseteq \Sigma^*$ be the desired and generated language under supervision, respectively. Prove that there exists a Σ_u-enabling, non-marking, and non-blocking supervisor S such that $L_m(G||S) = K_1$ and $L(G||S) = K_2$ if and only if.

1. $\overline{K_1} = K_2 \neq \emptyset$
2. K_1 is relative closed with respect to $L_m(G)$, and
3. K_2 is controllable.

Answer :

K_1 is $L_m(G)$-closed, then $K_1 = K_1 \cap L_m(G)K_2$ is $L_m(G)$-closed, then

$$K_2 = \overline{K_2} \cap L_m(G)$$
$$K_1 \cap K_2 = \overline{K_1} \cap L_m(G) \cap \overline{K_2} \cap L_m(G) = \overline{K_1} \cap \overline{K_2} \cap L_m(G)$$

So, $K_1 \cap K_2$ is $L_m(G)$-closed and controllable.

40 Let G be a trim automaton with $L_m(G) = (\alpha\gamma^*\beta)^*$. Let $K = (\alpha\beta)^*$ and $\Sigma_{uc} = \{\alpha, \beta\}$.

(a) Find a supervisor S such that $L_m(S/G) = K$ and check whether S is nonblocking;

(b) If we cannot find a nonblocking supervisor S such that $L_m(S/G) = K$, explain your reasoning;

(c) Portray $L_m(G)$ and K and use TCT to verify the reached conclusion.

Answer :
wait

41 Let $L(G) = \overline{\{u_1\alpha\gamma, u_1\alpha\beta, u_2\alpha\gamma\}}$, where $\Sigma = \Sigma_c$ and $E_{uo} = \{u_1, u_2\}$ (an event is controllable even if it is unobservable). (a) Let $K_1 = \overline{\{u_1\alpha\gamma, u_1\alpha\beta\}}$. Find, if possible, a (partially observable) supervisor S_P such that $L(S_P/G) = K_1$; (b) Let $K_2 = \overline{\{u_1\alpha\gamma, u_1\alpha\beta, u_2\alpha\}}$. Find, if possible, a (partially observable) supervisor S_P such that $L(S_P/G) = K_2$. Use TCT to verify the obtained results.

Answer : wait

42 Consider $\sigma = \{\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2\}$ and a string $s = \alpha_1\gamma_1\alpha_2\gamma_1$. Build an automaton G such that $L(G) = \Sigma^* \backslash \Sigma^*\{s\}\Sigma^*$. Analyze the reason why G satisfies the requirement.

Answer : wait

43 Suppose that a plant G has its alphabet $\Sigma = \{a_1, a_2, b_1, b_2, g_1, g_2\}$. Build another automaton that will generate the sublanguage of $L(G)$ where all the strings in $L(G)$ that contains the substrings $a_1a_2b_2$ or $a_1a_2g_2$ are removed.

Answer : wait

44 Consider a plant G with $L(G) = a^*b^*$ and the prefix-closed admissible language

Consider a plant G with $L(G) = a^*b^*$ and the prefix-closed admissible language is

$$L_a = \{a^n b^m \mid n \geq m \geq 0\}$$

Let the set of uncontrollable events be $E_{uc} = \{a\}$. Check if L_a is controllable and if it is a regular language.

Answer : wait

45 Given a plant G with $\Sigma_{uc} \subseteq \Sigma$ being the set of uncontrollable events and $K \subseteq \Sigma^*$.

Given a plant G with $\Sigma_{uc} \subseteq \Sigma$ being the set of uncontrollable events and $K \subseteq \Sigma^*$.Show the definition of controllability is equivalent to

$$\bar{K}\Sigma_{uc}^* \cap L(G) \subseteq \bar{K}$$

Answer : We know the defination of controllable Let $K \subseteq \Sigma^*(K = \emptyset)$. K is controllable with respect to G if

$$\bar{K}\Sigma_u \cap L(G) \subseteq \bar{K}$$
$$\bar{K}\Sigma_u = \{s \in \Sigma^* \mid s = s'\sigma, \sigma \in \Sigma_u, s' \in K\}$$

Equivalently, $(\forall s \in \Sigma^*)(\forall \sigma \in \Sigma)s \in K$ and $\sigma \in \Sigma_u$ and $s\sigma \in L(G) \Rightarrow s\sigma \in K$ For exmple $L_1 = \{\alpha\lambda\mu\}$ and $\overline{L_1} = \{\varepsilon, \alpha, \alpha\lambda, \alpha\lambda\mu\}$. L_1 is uncontrollable since $s = \alpha \in \bar{K}, \beta \in \Sigma_u, \alpha\beta \in L(G)[\alpha\beta \notin \bar{K}]$. For $s = \alpha, \sigma = \beta$ or λ Test $\lambda : \lambda\alpha \in K\,(\lambda \in \Sigma_u)$ controllable Test $\beta : \alpha\beta \notin L_1$ uncontrollable. Thus L_1 is uncontrollable.