One To Many Function

Trapdoor function science and cryptography, a trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction In theoretical computer science and cryptography, a trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are a special case of one-way functions and are widely used in public-key cryptography c3dc4a2ae5

Function (mathematics) mathematics, a function from a set X to a set Y assigns to each element of X exactly one element of Y. The set X is called the domain of the function and the In mathematics, a function from a set X to a set Y assigns to each element of X exactly one element of Y. The set X is called the domain of the function and the set Y is called the codomain of the function c3dc4a2ae5

One-to-many (data model), a type of relationship and cardinality in systems analysis c3dc4a2ae5 In mathematical terms, if f is a trapdoor function, then there exists some secret information t, such that given f(x) and t, it is easy to compute x. Consider a padlock and its key. It is trivial to change the padlock from open to closed without using the key, by pushing the shackle into the lock mechanism. Opening the padlock easily, however, requires the key to be used. Here the key t is the trapdoor and the padlock is the trapdoor function. c3dc4a2ae5 (c3dc4a2ae5 A homomorphism between algebraic structures is a function that is compatible with the operations of the structures. For all common algebraic structures, and, in particular for vector spaces, an injective homomorphism is also called a monomorphism. However, in the more general context of category theory, the definition of a monomorphism differs from that of an injective homomorphism. This is thus a theorem that they are equivalent for algebraic structures; see Homomorphism § Monomorphism for more details. c3dc4a2ae5

Loss function An optimization problem seeks to minimize a loss function.), in which case it is to be maximized. The loss function could include terms from several levels of the hierarchy. An objective function is either a loss function or its opposite (in specific domains, variously called a reward function, a profit function, a utility function, a fitness function, etc. theory, a loss function or

cost function (sometimes also called an error function) is a function that maps an event or values of one or more variables In mathematical optimization and decision theory, a loss function or cost function (sometimes also called an error function) is a function that maps an event or values of one or more variables onto a real number intuitively representing some "cost" associated with the event c3dc4a2ae5

Before the precise definition of computable functions, mathematicians often used the informal term effectively calculable. This term has since come to be identified with the computable functions. The effective computability... c3dc4a2ae5 In applied contexts, the terms "easy" and "hard" are usually interpreted relative to some specific computing entity; typically "cheap enough for the legitimate users" and "prohibitively expensive for any malicious agents". One-way functions, in this sense, are fundamental tools for cryptography, personal identification, authentication, and other data... c3dc4a2ae5

Cryptographic hash function A cryptographic hash function (CHF) is a hash algorithm (a map of an arbitrary binary string to a binary string with a fixed size of n {\displaystyle n} A cryptographic hash function (CHF) is a hash algorithm (a map of an arbitrary binary string to a binary string with a fixed size of c3dc4a2ae5

f c3dc4a2ae5

Computable function Only finitely many steps can be carried out before the value of the function is returned Computable functions are the basic objects of study in computability theory. Informally, a function is computable if there is an algorithm that computes the value of the function for every value of its argument. specific rule to cover what to do at each step of the calculation. Because of the lack of a precise definition of the concept of algorithm, every formal definition of computability must refer to a specific model of computation c3dc4a2ae5

A one to many relation, a relation such that at least one element of its domain is assigned to more than one elements of its codomain, and no element of its codomain is assigned to more than one element of its domain c3dc4a2ae5 n c3dc4a2ae5 Functions were originally the idealization of how a varying quantity depends on another quantity. For example, the position of a planet is a function of time. Historically, the concept was elaborated with the infinitesimal calculus at the end of the 17th century, and, until the 19th century, the functions that were considered were differentiable (that is, they

had a high degree of regularity). The concept of a function was formalized at the end of the 19th century in terms of set theory, and this greatly increased the possible applications of the concept. c3dc4a2ae5) c3dc4a2ae5

Multivalued function It is a set-valued function with additional properties depending on context; though some authors do not distinguish between set-valued functions and multifunctions. function, multiple-valued function, many-valued function, or multifunction, is a function that has two or more values in its range for at least one point In mathematics, a multivalued function, multiple-valued function, many-valued function, or multifunction, is a function that has two or more values in its range for at least one point in its domain c3dc4a2ae5

Multivalued function, a one-to-many function in mathematics c3dc4a2ae5 Many such models of computation have been proposed, the major ones being Turing machines, register machines, lambda calculus and general recursive functions. Although these four are of a very different nature, they provide exactly the same class of computable functions, and, for every model of computation that has ever been proposed, the computable functions for such a model are computable for the above four models of computation. c3dc4a2ae5 An example of a simple mathematical trapdoor is "6895601 is the product of two prime numbers. What are those numbers?" A typical "brute-force" solution would be to try dividing 6895601 by many prime numbers until finding the answer. However, if one is told that 1931 is one of the numbers, one can find the answer by entering "6895601 ÷ 1931" into any calculator. This example is not a sturdy trapdoor... c3dc4a2ae5

One-way function). science Do one-way functions exist. (See § Theoretical definition, below. More unsolved problems in computer science In computer science, a one-way function is a function that is easy to compute In computer science, a one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. This has nothing to do with whether the function is one-to-one; finding any one input with the desired image is considered a successful inversion. Here, "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems c3dc4a2ae5

In statistics, typically a loss function is used for parameter estimation, and the event in question is some function of the difference between estimated and true values for an instance of data. The concept, as old as Laplace, was reintroduced in statistics by Abraham Wald in the middle of the 20th century. In the context of economics, for example, this is usually economic cost or

regret. In classification, it is the penalty for an incorrect classification of an example. In actuarial science, it is used in an insurance context to model benefits paid over premiums... c3dc4a2ae5 Point-to-multipoint communication, communication which has a one-to-many relationship c3dc4a2ae5 A multivalued function of sets f : X → Y is a subset c3dc4a2ae5 x c3dc4a2ae5

Injective function In other words, every element of the function's codomain is the image of at most one element of its domain. The term one-to-one function must not be confused with one-to-one correspondence that refers to bijective functions, which are functions such that each element in the codomain is an image of exactly one element in the domain. an injective function (also known as injection, or one-to-one function) is a function f that maps distinct elements of its domain to distinct elements In mathematics, an injective function (also known as injection, or one-to-one function) is a function f that maps distinct elements of its domain to distinct elements of its codomain; that is, x1 ≠ x2 implies f(x1) ≠ f(x2) (equivalently by contraposition, f(x1) = f(x2) implies x1 = x2) c3dc4a2ae5

Γ c3dc4a2ae5

One-to-many up one-to-many in Wiktionary, the free dictionary. One-to-many may refer to: Fat link, a one-to-many link in hypertext Multivalued function, a one-to-many One-to-many may refer to: c3dc4a2ae5

A function c3dc4a2ae5 A function is often denoted by a letter such as f, g or h. The value of a function f at an element x of its domain (that is, the element of the codomain that is associated with x) is denoted by f(x); for example, the value of f at x = 4 is denoted by f(4). Commonly, a specific function is defined by means of an expression depending on x, such as c3dc4a2ae5 Fat link, a one-to-many link in hypertext c3dc4a2ae5 The existence of such one-way functions is still an open conjecture. Their existence would prove that the complexity classes P and NP are not equal, thus resolving the foremost unsolved question of theoretical computer science. The converse is not known to be true, i.e. the existence of a proof that P ≠ NP would not directly imply the existence of one-way functions. c3dc4a2ae5 =... c3dc4a2ae5 L c3dc4a2ae5

Many-one reduction {\displaystyle B}. If such a function f {\displaystyle f} exists, one says that A {\displaystyle A} is many-one reducible or m-reducible to B {\displaystyle B} In computability theory and computational complexity theory, a many-one reduction (also called mapping reduction) is a reduction

that converts instances of one decision problem (whether an instance is in c3dc4a2ae5

The Church–Turing thesis is the unprovable assertion that every notion of computability that can be imagined can compute only functions that are computable in the above sense. c3dc4a2ae5 f c3dc4a2ae5