

22 | new Function('x = 100')();: 函数的类化是对动态与静态系统的再次统一

2020-01-03 周爱民

《JavaScript核心原理解析》

[课程介绍 >](#)



讲述：周爱民

时长 14:58 大小 12.00M



你好，我是周爱民，欢迎回到我的专栏。

今天是专栏最后一讲，我接下来要跟你聊的，仍然是 JavaScript 的动态语言特性，主要是动态函数的实现原理。

标题中的代码比较简单，是常用、常见的。这里稍微需要强调一下的是“最后一对括号的使用”，由于运算符优先级的设计，它是在 new 运算之后才被调用的。也就是说，标题中的代码等义于：

```
1 // （等义于）
2 (new Function('x = 100'))()
3
4 // （或）
```

 复制代码



```
5 f = new Function('x = 100')
6 f()
```

此外，这里的new运算符也可以去掉。也就是说：

```
1 new Function(x)
2
3 // vs.
4 Function(x)
```

 复制代码

这两种写法没有区别，都是动态地创建一个函数。

函数的动态创建

如果在代码中声明一个函数，那么这个函数必然是具名的。具名的、静态的函数声明有两个特性：

1. 是它在所有代码运行之前被创建；
2. 它作为语句的执行结果将是“空（Empty）”。

这是早期 JavaScript 中的一个硬性的约定，但是到了 ECMAScript 6 开始支持模块的时候，这个设计就成了问题。因为模块是静态装配的，这意味着它导出的内容“应该是”**一个声明的结果或者一个声明的名字**，因为只有**声明**才是静态装配阶段的特性。但是，所有声明语句的完成结果都是 Empty，是无效的，不能用于导出。

NOTE：关于 6 种声明，请参见《[第 02 讲](#)》。

而声明的名字呢？不错，这对具名函数来说没问题。但是匿名函数呢？就成了问题了。

因此，在支持匿名函数的“缺省导出（export default ...）”时，ECMAScript 就引入了一个称为“函数定义（Function Definitions）”的概念。这种情况下，函数表达式是匿名的，但它的结果会绑定给一个名字，并且最终会导出那个名字。这样一来，函数表达式也就有了“类似声明的性质”，但它又不是静态声明（Declarations），所以概念上叫做定义（Definitions）。



NOTE：关于匿名函数对缺省导出的影响，参见《[第 04 讲](#)》。

在静态声明的函数、类，以及这里说到的函数定义之外，用户代码还可以创建自己的函数。这同样有好几种方式，其中之一，是使用`eval()`，例如：

复制代码

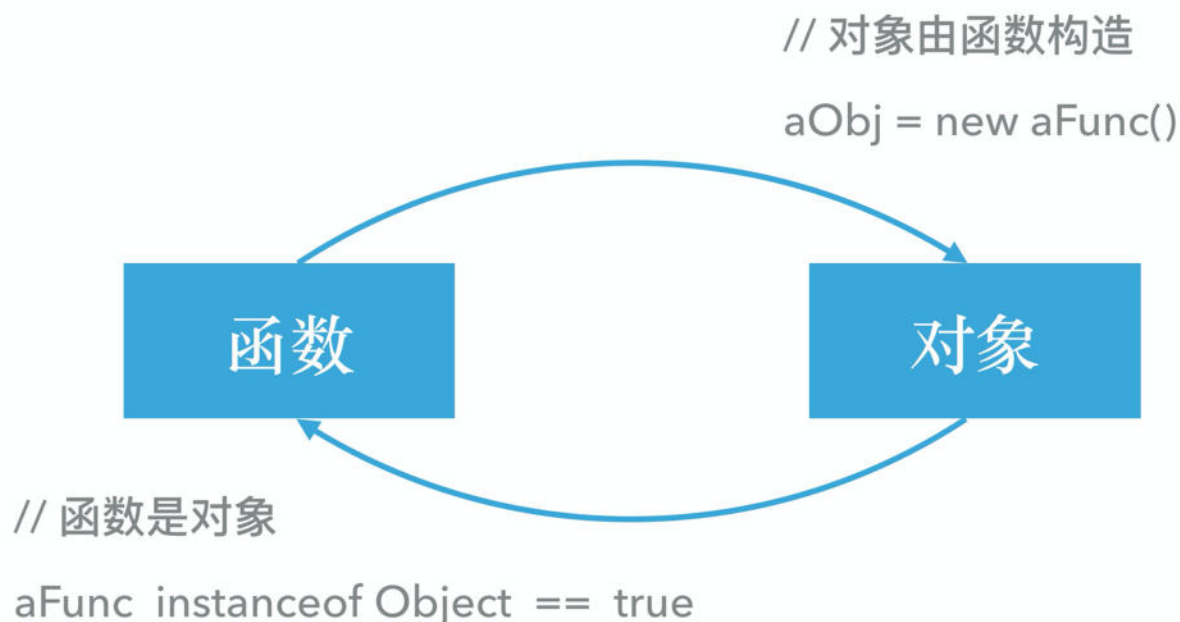
```
1 # 在非严格模式下，这将在当前上下文中“声明”一个名为foo的函数
2 > eval('function foo() {}')
```

还有一种常见的方式，就是使用动态创建。

几种动态函数的构造器

在 JavaScript 中，“动态创建”一个东西，意味着这个东西是一个对象，它创建自类 / 构造器。其中`Function()`是一切函数缺省的构造器（或类）。尽管内建函数并不创建自它，但所有的内建函数也通过简单的映射将它们的原型指向 `Function`。除非经过特殊的处理，所有 JavaScript 中的函数原型均最终指向`Function()`，它是所有函数的祖先类。

这种处理 / 设计使得 JavaScript 中的函数有了“完整的”面向对象特性，函数的“类化”实现了 JavaScript 在函数式语言和面向对象语言在概念上的大一统。于是，一个内核级别的概念完整性出现了，也就是所谓：对象创建自函数；函数是对象。如下图所示：



NOTE：关于概念完整性以及它在“体系性”中的价值，参见《[🍷加餐 3：让 JavaScript 运行起来](#)》。

在 ECMAScript 6 之后，有赖于类继承体系的提出，JavaScript 中的函数也获得了“子类化”的能力，于是用户代码也可以派生函数的子类了。例如：

```
1 class MyFunction extends Function {  
2   // ...  
3 }
```

 复制代码

但是用户代码无法重载“函数的执行”能力。很明显，这是执行引擎自身的能力，除非你可以重写引擎，否则重载执行能力也就无从谈起。

NOTE：关于类、派生，以及它们在对原生构造器进行派生时的贡献，请参见《[🍷第 15 讲](#)》。

除了这种用户自定义的子类化的函数之外，JavaScript 中一共只有四种可以动态创建的函数，包括：**一般函数**（Function）、**生成器函数**（GeneratorFunction）、**异步生成器函数**（AsyncGeneratorFunction）和**异步函数**（AsyncFunction）。又或者说，用户代码可以从这四种函数之任一开始来派生它们的子类，在保留它们的执行能力的同时，扩展接口或功能。

但是，这四种函数在 JavaScript 中有且只有Function()是显式声明的，其他三种都没有直接声明它们的构造器，这需要你如下代码来得到：

```
1 const GeneratorFunction = (function* (){}).constructor;  
2 const AsyncGeneratorFunction = (async function* (){}).constructor  
3 const AsyncFunction = (async x=>x).constructor;  
4  
5 // 示例  
6 (new AsyncFunction)().then(console.log); // promise print 'undefined'
```

 复制代码

函数的三个组件



我们提及过函数的三个组件，包括：**参数**、**执行体**和**结果**。其中“结果（Result）”是由代码中的 `return` 子句负责的，而其他两个组件，则是“动态创建一个函数”所必须的。这也是上述四个函数（以及它们的子类）拥有如下相同界面的原因：

`Function (p1, p2, ... , pn, body)`

NOTE：关于函数的三个组件，以及基于它们的变化，请参见《[第 8 讲](#)、[第 9 讲](#)、[第 10 讲](#)，它们分别讨论“三个组件”、改造“执行体”，以及改造“参数和结果”》。

其中，用户代码可以使用字符串来指定 `p1...pn` 的形式参数（Formals），并且使用字符串来指定函数的执行体（Body）。类似如下：

```
1 f = new Function('x', 'y', 'z', 'console.log(x, y, z)');
2
3 // 测试
4 f(1,2,3); // 1 2 3
```

 复制代码


JavaScript 也允许用户代码将多个参数合写为一个，也就是变成类似如下形式：

```
1 f = new Function('x, y, z', ...);
```

 复制代码

或者在字符串声明中使用缺省参数等扩展风格，例如：

```
1 f = new Function('x = 0, ...args', 'console.log(x, ...args)');
2 f(undefined, 200, 300, 400); // 0 200 300 400
```

 复制代码

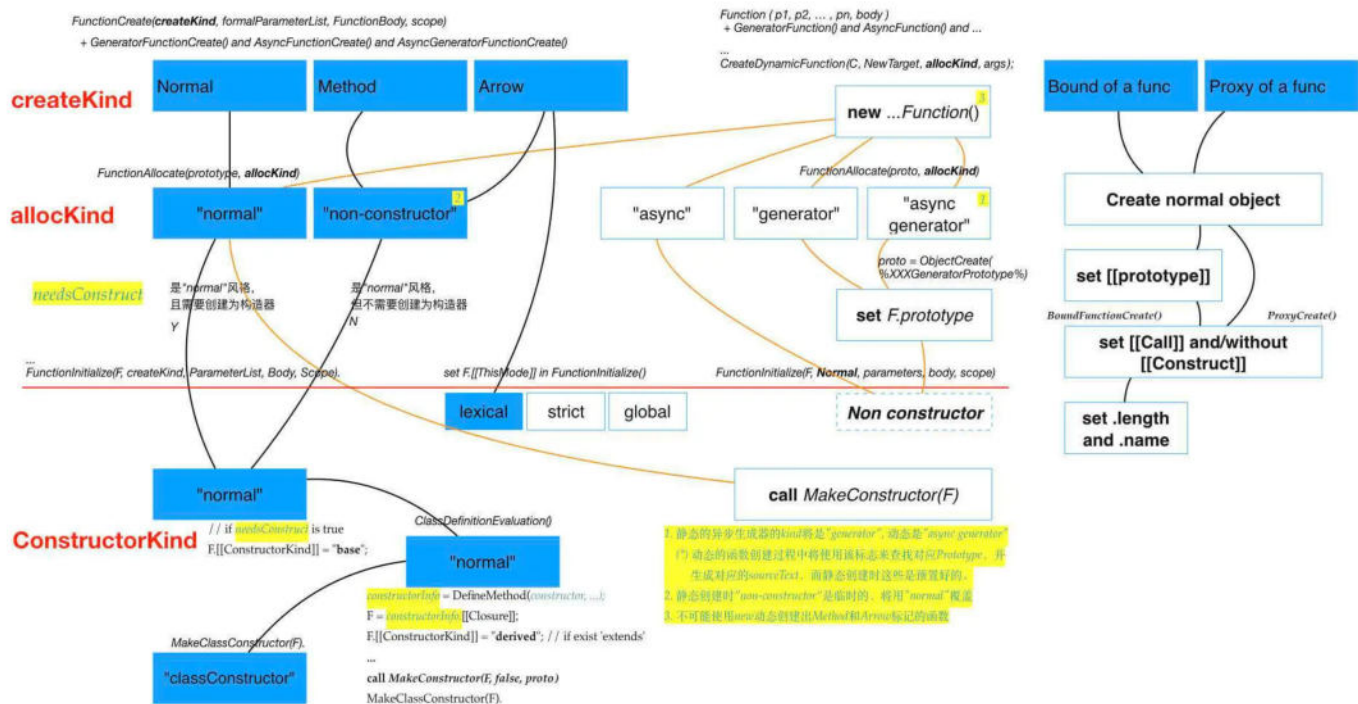
动态函数的创建过程

所有的四种动态函数的创建过程都是一致的，它们都将调用内部过程

[CreateDynamicFunction\(\)](#)来创建函数对象。但相对于静态声明的函数，动态创建（CreateDynamicFunction）却有自己不同的特点与实现过程。



NOTE: 关于对象的构造过程, 请参见《第 13 讲 (13 | new X)》。



JavaScript 在创建函数对象时, 会为它分配一个称为“allocKind”的标识。相对于静态创建, 这个标识在动态创建过程中反而更加简单, 正好与上述四种构造器——对应, 也就不再需要进行语法级别的分析与识别。其中除了normal类型（它所对应的构造器是Function()）之外, 其他的三种都不能作为构造器来创建和初始化。所以, 只需要简单地填写它们的内部槽, 并置相应的原型（原型属性 F.prototype 以及内部槽 F.[[Prototype]]）就可以了。

最后, 当函数作为对象实例完成创建之后, 引擎会调用一个称为“函数初始化（FunctionInitialize）”的内置过程, 来初始那些与具体实例相关的内部槽和外部属性。

NOTE: 在 ECMAScript 6 中, 动态函数的创建过程主要由 FunctionAllocate 和 FunctionInitialize 两个阶段完成。而到了 ECMAScript 9 中, ECMAScript 规范将 FunctionAllocate 的主要功能归入到 OrdinaryFunctionCreate 中（并由此规范了函数“作为对象”的创建过程）, 而原本由 FunctionInitialize 负责的初始化, 则直接在动态创建过程中处理了。

然后呢? 然后, 函数就创建完了。

是的! “好像”什么也没有发生? ! 事实上, 在引擎层面, 所谓的“动态函数创建”就是什么也没有发生, 因为执行引擎并不理解“声明一个函数”与“动态创建一个函数”之间的差异。



我们试想一下，如果一个执行引擎要分别理解这两种函数并尝试不同的执行模式或逻辑，那么这个引擎的效率得有多差。

作为一个函数

通常情况下，接下来还需要一个变量来引用这个函数对象，或者将它作为表达式操作数，它才会有意义。如果它作为引用，那么它跟普通变量或其他类型的数据类似；如果它作为一般操作数，那么它应该按照上一讲所说的规则，转换成“值类型”才能进行运算。

NOTE：关于引用、操作数，以及值类型等等，请参见《[第 01 讲 \(01 | delete 0\)](#)》。

所以，如果不讨论“动态函数创建”内在的特殊性，那么它的创建与其他数据并没有本质的不同：创建结果一样，对执行引擎或运行环境的影响也一样。而这种“没有差异”反而体现了“函数式语言”的一项基本特性：函数是数据。也就是说，函数可以作为一般数据来处理，例如对象，又例如值。

函数与其他数据不同之处，仅在于它是可以调用的。那么“动态创建的函数”与一般函数相比较，在调用 / 执行方面有什么特殊性吗？

答案是，仍然没有！在 ECMAScript 的内部方法 `call()` 或者函数对象的内部槽 `[[Call]]` `[[Construct]]` 中，根本没有任何代码来区别这两种方式创建出来的函数。它们之间毫无差异。

NOTE：事实上，不惟如此，我尝试过很多的方式来识别不同类型的函数（例如构造器、类、方法等）。除了极少的特例之外，在用户代码层面是没有办法识别函数的类型的。就现在的进展而言，`isBindable()`、`isCallable()`、`isConstructor()` 和 `isProxy()` 这四个函数是可以实现的，其他的类似 `isClassConstructor()`、`isMethod()` 和 `isArrowFunction()` 都没有有效的识别方式。

NOTE：如上的这些识别函数，需要在不利用 `toString()` 方法，以及不调用函数的情况下来完成。因为执行函数会带来未知的结果，而 `toString` 方法的实现在许多引擎中并不标准，不可依赖。



不过，如果我们将时钟往回拨一点，考察一下这个函数被创建出来之前所发生的事情，那么，我们还是能找到“唯一一点不同”。而这，也将是我在“动态语言”这个系列中为你揭示的最后一

个秘密。

唯一一点不同

在“函数初始化（FunctionInitialize）”这个阶段中，ECMAScript 破天荒地约定了几行代码，这段规范文字如下：

```
Let realmF be the value of F's [[Realm]] internal slot.  
Let scope be realmF. [[GlobalEnv]].  
Perform FunctionInitialize(F, Normal, parameters, body, scope).
```

它们是什么意思呢？

规范约定需要从函数对象所在的“域（即引擎的一个实例）”中取出全局环境，然后将它作为“父级的作用域（scope）”，传入FunctionInitialize()来初始化函数F。也就是说，所有的“动态函数”的父级作用域将指向全局！

你绝不可能在“当前上下文（环境 / 作用域）”中动态创建动态函数。和间接调用模式下的eval()一样，所有动态函数都将创建在全局！

一说到跟“间接调用 eval()”存有的相似之处，可能你立即会反应过来：这种情况下，eval()不仅仅是在全局执行，而且将突破“全局的严格模式”，代码将执行在非严格模式中！那么，是不是说，“动态函数”既然与它有相似之处，是不是也有类似性质呢？

NOTE：关于间接调用eval()，请参见《[第 21 讲](#)》。

答案是：的确！

出于与“间接调用 eval()”相同的原因——即，在动态执行过程中无法有效地（通过上下文和对应的环境）检测全局的严格模式状态，所以动态函数在创建时只检测代码文本中的第一行代码是否为use strict指示字，而忽略它“外部 scope”是否处于严格模式中。

因此，即使你在严格模式的全局环境中创建动态函数，它也是执行在非严格模式中的。它与“间接调用 eval()”的唯一差异，仅在于“多封装了一层函数”。



例如：

 复制代码

```
1 # 让NodeJS在启动严格模式的全局
2 > node --use-strict
3
4 # （在上例启动的NodeJS环境中测试）
5 > x = "Hi"
6 ReferenceError: x is not defined
7
8 # 执行在全局，没有异常
9 > new Function('x = "Hi"')()
10 undefined
11
12 # `x` 被创建
13 > x
14 'Hi'
15
16 # 使用间接调用的`eval`来创建`y`
17 > (0, eval)('y = "Hello"')
18 > y
19 'Hello'
```

结尾

所以，回到今天这一讲的标题上来。标题中的代码，事实与上一讲中提到的“间接调用eval()”的效果一致，同样也会因为在全局中“向未声明变量赋值”而导致创建一个新的变量名x。并且，这一效果同样不受所谓的“严格模式”的影响。

在 JavaScript 的执行系统中出现这两个语法效果的根本原因，在于执行系统试图从语法环境中独立出来。如果考虑具体环境的差异性，那么执行引擎的性能将会较差，且不易优化；如果不考虑这种差异性，那么“严格模式”这样的性质就不能作为（执行引擎理解的）环境属性。

在这个两难中，ECMAScript 帮助我们做出了选择：牺牲一致性，换取性能。

NOTE：关于间接调用eval()对环境的使用，以及环境相关的执行引擎组件的设计与限制，请参见《[第 20 讲](#)》。



当然这也带来了另外一些好处。例如终于有了window.execScript()的替代实现，以及通过new Function这样来得到的、动态创建的函数，就可以“安全地”应用于并发环境。

至于现在，《JavaScript 核心原理解析》一共 22 讲内容就全部结束了。

在这个专栏中，我为你讲述了 JavaScript 的静态语言设计、面向对象语言的基本特性，以及动态语言中的类型与执行系统。这看起来是一些零碎的、基本的，以及应用性不强的 JavaScript 特性，但是事实上，它们是你理解“更加深入的核心原理”的基础。

如果不先掌握这些内容，那么更深入的，例如多线程、并行语言特性等等都是空中楼阁，就算你勉强学来，也不过是花架子，是理解不到真正的“核心”的。

而这也是我像现在这样设计《JavaScript 核心原理解析》22 讲框架的原因。我希望你能在这些方面打个基础，先理解一下 ECMAScript 作为“语言设计者”这个角色的职责和关注点，先尝试一下深入探索 JavaScript 核心原理的乐趣（与艰难）。然后，希望我们还有机会在新的课程中再见！

＝ 在 1 月 13 日前提交问卷，将有机会 ＝

得

极客时间
超大鼠标垫



或得

极客时间课程阅码
价值 ¥99



多谢你的收听，最后邀请你填写这个专栏的 [📝 调查问卷](#)，我也想听听你的意见和建议，我将继续答疑解惑、查漏补缺，与你回顾这一路行来的苦乐。



再见。

NOTE：编辑同学说还有一个“结束语”，我真不知道怎么写。不过，如果你觉得意犹未尽的话，到时候请打开听听吧（或许还有好货吖）。

by aimgoo.

分享给需要的人，Ta购买本课程，你将得 20 元

生成海报并分享

赞 1 提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

- 上一篇 21 | (0, eval)("x = 100")：一行让严格模式形同虚设的破坏性设计（下）
- 下一篇 结束语 | 愿你能做一个真正“懂”的程序员

学习推荐

JVM + NIO + Spring

各大厂面试题及知识点详解

限时免费





独钓寒江雪
2020-01-03

今天读完了专栏必学内容的最后一讲，跟着老师的步伐一路走来，很艰辛，同时也收获很多，通过一行极简的代码去洞悉一门语言的核心原理，也是我一直梦想着能做到的事，向老师致敬！

其实，可以说，看这种底层的东西，每一讲都很吃力，要想有更深入的理解，必须再花时间回过头反复研读；其实，阅读专栏，很多时候也是一种思维的提升，比如以前只知道变量提升，却没想过为什么要提升；知道...运算符，却说不出为什么可以用它来展开对象。。。

或许专栏短期内对开发能力不会有多么显著的提升，但我相信，因为对语言本质的洞悉而产生的自信以及思想层面的提升，将会使我在前端走的更远。衷心的感谢🙏

作者回复: 🙏



👍 6



行问
2020-01-03

`new Function(x)` vs `Function(x)` 没什么区别。如果是“类化”的话，也是没什么区别吗？在使用 `class` 声明一个类时，`new class` 与 `class` 直接调用。

函数是对象的概念比较清晰，明了。这让我想起之前的 "null"，请教个问题，在通常的开发中，会把一些变量释放空间，把值置为 `null`，那么如果是置为 `{}` 呢？如下：

`var a = null` 和 `var a = {}`，是否有大差异？

我的理解是 `{}` 会存放在“堆空间”占据内存，但同时它是一个空对象，`null` 也是一个什么都没有的空对象，但 `null` 也是其它对象的原型，所以也会有 `Object.create(null)`

不知道周大能否看懂我的逻辑？

感谢

作者回复: Oh. 这个

> `new Function(x)` vs `Function(x)` 没什么区别



并不算是很特别的特例。你应该记得new AClass()的时候，允许“用户代码直接返回对象，而不是直接使用this”

这个特性对吧，其实这就是这个特性的应用。因为当用户代码返回自己创建的对象是，用不用new，效果都是一样的了。——所以，这里的意思是说，Function()在实现时也是自己返回了对象，而没有使用缺省new给他创建的this。

理论上，这对类化来说也是适用的。因为类化也允许用户代码返回对象来替代this。但是——呵呵，如果你用“class X...”来声明类，那么这个X是只能用new来调用的，而不能直接当做函数调用。

```
...
```

```
> X()
```

```
TypeError: Class constructor X cannot be invoked without 'new'
```

```
...
```

关于null值和{}。其实null值是一个特殊性，它是真的“什么也没有”，你甚至可以将它理解为C里面的#0。而它是对象（typeof null），以及它能作为其它对象或类的原型，只是一个语言设计，而与它的内存占用没有关系。你可以这样理解，没问题。——另外，在ECMAScript中，null是一个原始值（Primitive value），这意味着它可以直接在引擎中表达为二进制的存储，真的跟#0很接近了。^^.

而{}是一个对象，它在引擎中表达为一个结构、一个数据块（也就是你认为的放在堆里，其实是不是放在堆里不重要，而且也并不确定）。对象之所以为空白（“{}”称为空白对象Empty objects），是因为它的自有属性表为空，当自有属性表里面没有属性项的时候，它就是空白的了。——你可以重置它的原型，让他表现得有一些属性什么的。因为它毕竟还是一个可操作的、占有引擎中的存储的真实对象。

另外，ECMAScript内部（以及引擎内部的执行逻辑中）其实是把null值理解为“值”的，而不是“对象”。所以ECMAScript的内部方法isObject(null)，是返回false的。

共 2 条评论 >



4



晓小东

2020-01-03

好快，这个专栏结束了，有点舍不得，一个多月来我一直关注老师更新，反复阅听之前章节。体会深思理解，发现如果没有老师带领层层分析JavaScript 最核心那部分设计和概念，真的无缘了解这门语言了，谢谢老师给我们思维上的提升，同时也发现自己对这门语言的理解上，上了一个大大的台阶。在此由衷的感谢，真的感觉，遇到了恩师。

作者回复: 😊+👏



2



weineel

2020-01-05

老师的每一篇都很有深度。我们平时开发中，this 的动态绑定虽然很复杂，但时间长了也能找到规律，仅仅是应用还是没啥问题的。老师要是有时间给我们加个餐，聊聊 this 的深层原理吧。

作者回复: 这个可以有。我考虑一下怎么做到下一个课程吧。这一课结束啦所以也不再有加餐啦。^^.



大雄不爱吃肉

2021-04-01

专栏虽然是二十多讲，但是自己看了很久，很多地方反复看反复试。可能最终记住的不是很多，但对js以及语言规范有了深刻的理解，感谢老师这门课，这一门独特的课程我收获颇多，期待老师的下一门课！

作者回复: 多谢多谢。有收获就好。:)



igetter

2020-06-14

老师，问一个不太相关的问题: MDN中说，Function()比eval()更高效。这是真的吗？

作者回复: 是的。

Function(x)工作在全局，所以它的作用域层次通常要小于eval(x)。因为作用域（链）的深度小，所以Function()执行要略高效。

如果只是说对代码文本`x`的解析和处理等，两者并没有明显的性能区别。



K4SHIFZ

2020-05-03

动态函数创建在规范19.2.1.1.1

Let proto be ? GetPrototypeFromConstructor(newTarget, fallbackProto).

Let realmF be the current Realm Record.

Let scope be realmF.[[GlobalEnv]].

Let F be ! OrdinaryFunctionCreate(proto, sourceText, parameters, body, non-lexical-this, scope).

Perform SetFunctionName(F, "anonymous")





James

2020-02-05

老师，我从头听了一遍，有几篇文章听了好几遍，但是感觉完全是云里雾里，没弄懂。我应该怎么办。😓

作者回复: 补一些基础，再看。建议边读ECMAScript边看。加餐里面我有给地址～找找哇😊

共 2 条评论 >



许童童

2020-01-04

一路跟着老师走过来，自以为对JavaScript这门语言有一定的了解，才发现只是懂点皮毛，更多深入的知识自己都还没有探究到，感谢老师带我领会了更深刻的JavaScript。之后还是会持续学习，保持对JavaScript的敬畏之心，加油。

作者回复: 能对大家有用就好。我一直以这样的态度来做这件事，那怕能帮助一人，也是好的。多谢你的支持。^^.



独钓寒江雪

2020-01-03

以前有碰到了这样一个疑惑，看了专栏前面的内容，还是不太明白。下面是我的代码，虽然问题比较好解决，但是不太明白：

```
import { message } from 'antd' // 引入AntD组件库中的message
export const generateRemark = (skus, message) => { // 这个方法被导出，接收两个参数，其中一个写成了message
  let remark = ''
  .....
  remark = remark + (message || '') // 使用了message参数
  return remark
}
```

当我调用generateRemark(skus, '')时（message传入的是空字符串），返回是[object Object],调试发现，原来message被解析成了antd的message组件了。

是代码环境的问题还是JS底层机制的问题呢？希望老师能帮我解惑，谢谢🙏



最后，也感谢老师的专栏，这样关注底层核心原理的专栏，正是我这种自学前端出道的同学所需要的。

作者回复: 仔细阅读了几遍你的问题, 我觉得这是不可能出现的。但还是小心地写了一个测试来运行了一下, 但是还原不了你说的问题。(代码放在后面, 你看看是不是这个意思)

我仔细想了一下, 非常可疑的事情出来你使用import/export的方法上面。由于NodeJS在一般模式下并不支持ES Module, 因此通常我们在应用环境中使用模块的时候, 都是用babel来转码的。而早期babel (也包括其它的一些第三方转码器) 可能对某些语法支持得不好, 所以转出来的结果跟ECMAScript规范并不一致, 做不到百分百地兼容。并且, 在你的示例中还有一个箭头函数, 这个东西在很多转码器和基于转码器的runtime中还是实现得不好的。

所以简单地说, 我怀疑是你在应用环境中使用babel或typescript之类的转码器带来的结果。无论如何, ECMAScript的规范中不会有这个问题。如下例:

```
...

# 运行
> node --experimental-modules t1.mjs

// 代码t1.mjs
import { generateRemark } from './t2.mjs';

var skus = '';
console.log(generateRemark(skus, ''));

// 代码t2.mjs
import { message } from './t3.mjs'

export const generateRemark = (skus, message) => {
  let remark = ''
  // .....
  console.log(typeof message, message);

  remark = remark + (message || '')
  return remark
}

// 代码t3.mjs
export var message = {};
...
```



