Repair Proxy Transparency

Mark S. Miller, Caridy Patino, Keith Miller, Tom Van Cutsem

TC39 November 2017

[?,ES5]

```
> const x = {}, y = {};
> x.__proto__ = y;
> y.__proto__ = x;
TypeError: Cyclic __proto__ value
```

No `__proto__` or mutable prototype in ES5.

But proto mutation not prohibited in ES5.

Proto mutation that would create cycles must throw.

Thus, proto cycles impossible.

Cycle check is atomic, by reading [[Prototype]] properties

ES6

```
> const p = Proxy(…), q = new Proxy(…);
> p.__proto__ = q;
> q.__proto__ = p;
```

Prototype chain is behavior, not data.

At the time, we found no `setPrototype` restriction

that would ensure `getPrototype` calls do not report a cycle

Instead, just dropped the cycle check.

ES6

```
> const x = {}, y = {};
> x.__proto__ = y;
> y.__proto__ = x;
```

Prototype chain is behavior, not data.

At the time, we found no `setPrototype` restriction

that would ensure `getPrototype` calls do not report a cycle

Instead, just dropped the cycle check everywhere.

Preserve proxy transparency: `p` can act like `x`

(ES6,now]

```
> const p = Proxy(…), q = new Proxy(…);
> p.__proto__ = q;
> q.__proto__ = p;

> const x = {}, y = {};
> x.__proto__ = y;
> y.__proto__ = x;
TypeError: Cyclic __proto__ value
```

Can detect a proxy that wishes to be seem non-exotic.

What needs repair?

Threat: Detect a proxy that wishes to seem non-exotic.

A proxy that wants to, can behave like only an exotic can.

Only proxies that want to be undetectable need to be undetectable.

Needed restriction must be non-onerous. Membranes must still work.

Spectrum of Options

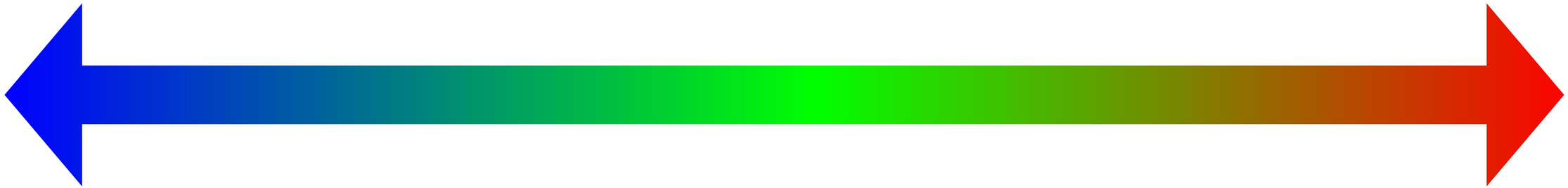
Lazy sample all traps

Lazy sample frozen traps

Pre-sample frozen `getPrototypeOf`

Pre-sample all traps

Pre-sample frozen traps



Easier High Performance

Don’t break old handlers

Pre-sample all traps

```
const p = new Proxy(target, handler);
```

Doing a [[Get]] on handler is like [[Get]]ing ‘`next`’ on iterator.

Instead, treat handler as a bag of named arguments.

[[Get]] the trap functions only during Proxy construction.

Bigger win: Absent trap functions —> specialize proxy onto target

Break web? Old self-mutating handlers break

Atomic Cycle Check Through Proxies