COLLABORA

TOP SECRET

CONFIDENTIAL

COLLABORA

~~TOP SECRET~~

WITCHCRAFT SECRETS

~~CONFIDENTIAL~~

Witchcraft Secrets

...from a reverse-engineer

Alyssa Rosenzweig

Starswirl's First Law

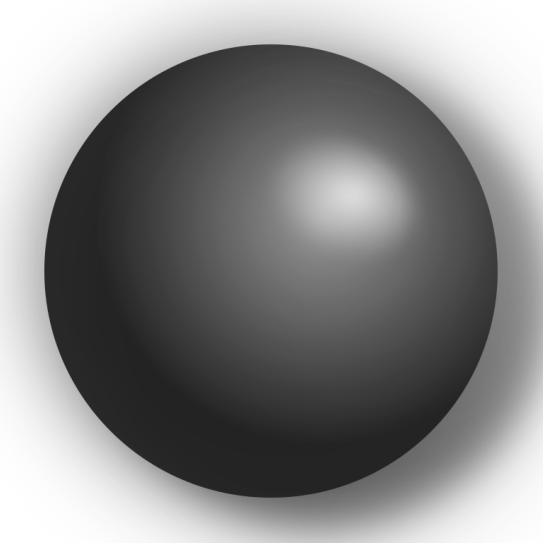
Magic can neither be created nor destroyed...

Starswirl's First Law

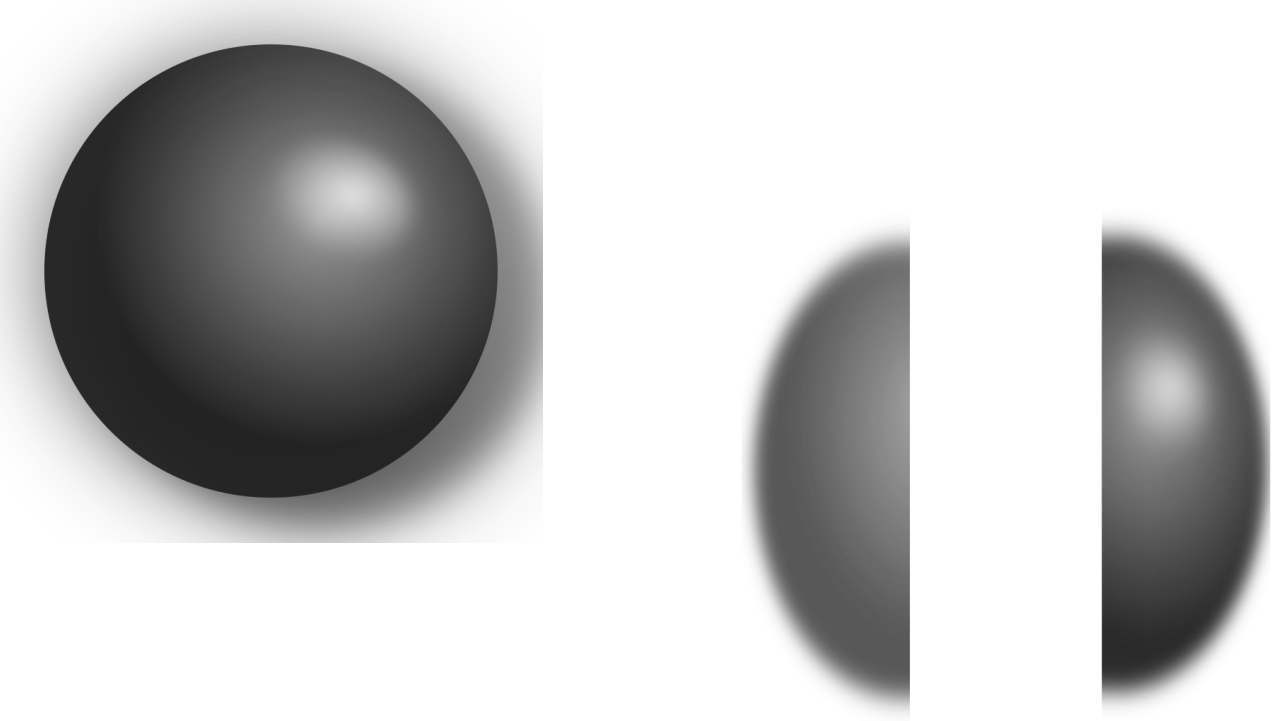
Magic can neither be created nor destroyed...

....only transformed.

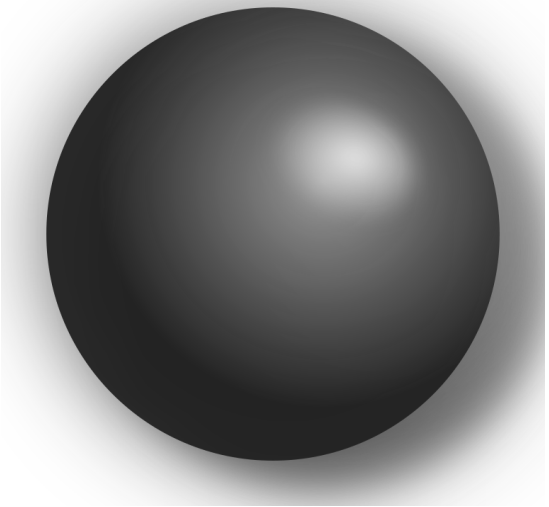
Starswirl’s First Law

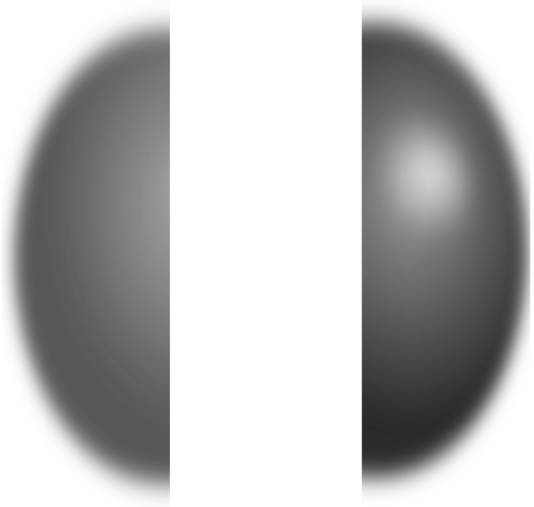


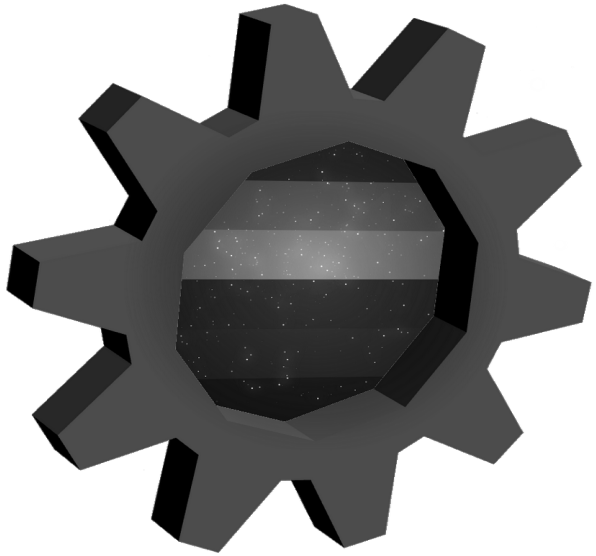
Starswirl’s First Law



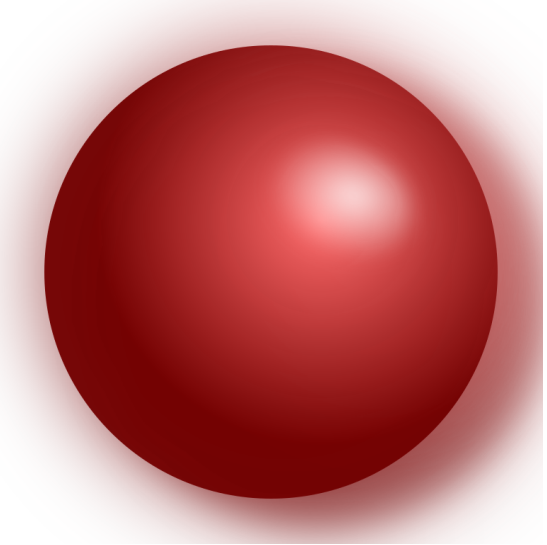
Starswirl’s First Law

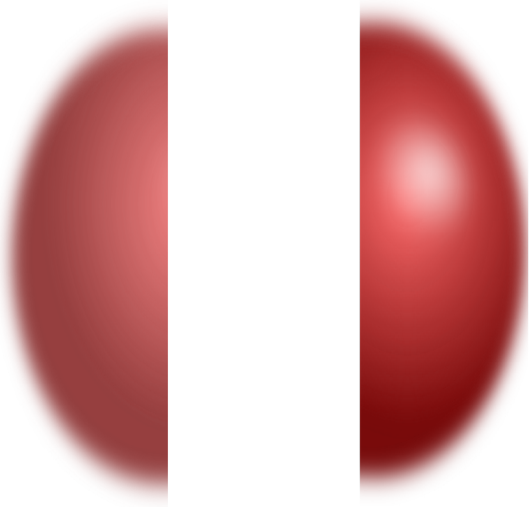


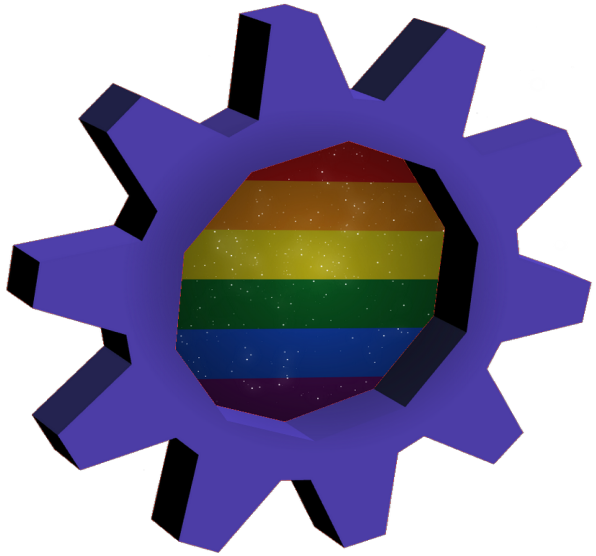




Witchcraft







COLLABORA

OPEN SORCERY

COLLABORA

STEPS

Steps - trivial

- Write a test
- Trace baseline input
- Trace with single “interesting” change
- Diff the traces
- Single change? Lucky.

Spelling convention

$$f(x) = y$$

Steps - nontrivial

- Write a test
- Trace many inputs
- Record results
- Find a pattern
- Deduce f
- Rewrite for f^{-1}

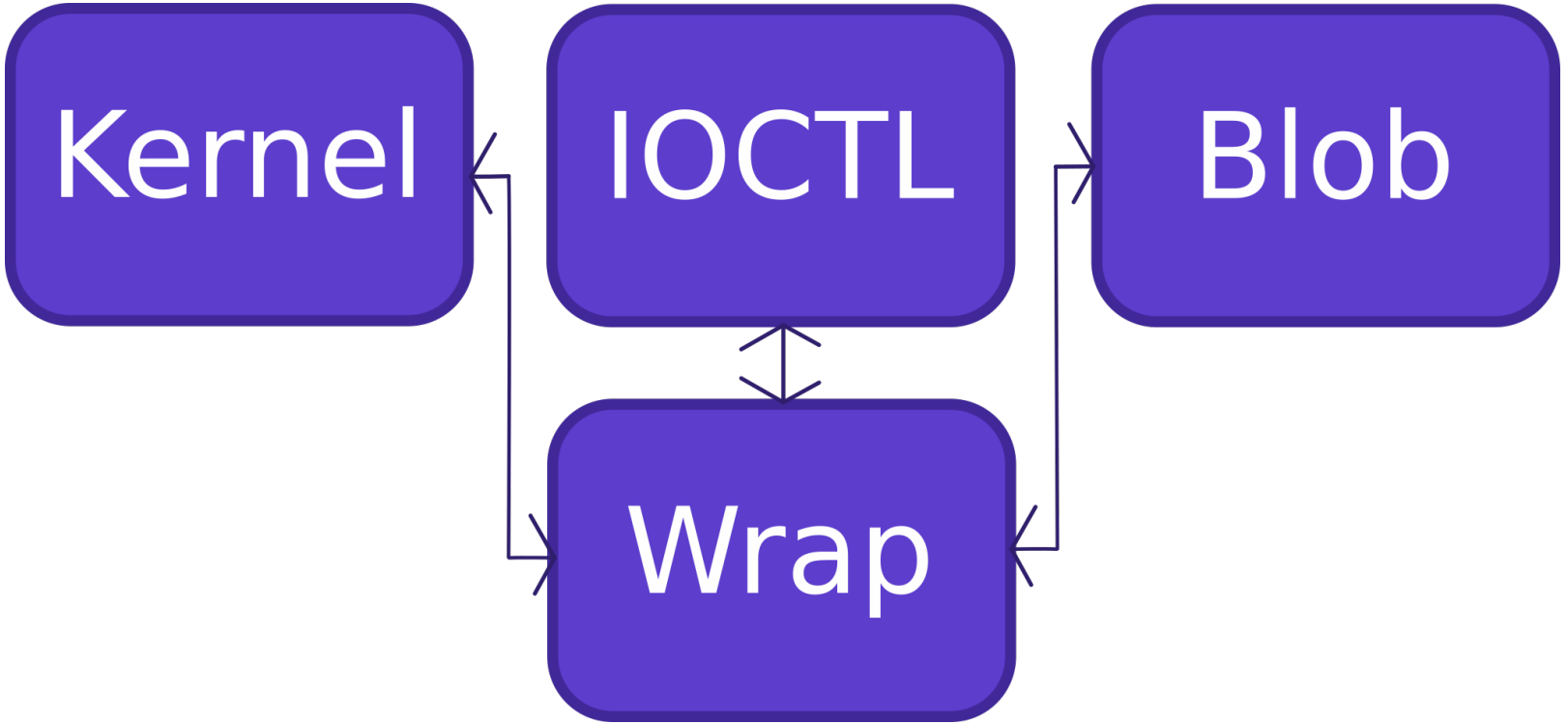
Steps - nontrivial

- Write a test
- **Trace many inputs**
- Record results
- Find a pattern
- Deduce f
- Rewrite for f^{-1}

COLLABORA

TRACING


Kernel
IOCTL
Blob


Kernel
IOCTL
Blob
Wrap

Steps - nontrivial

- Write a test
- Trace many inputs
- Record results
- **Find a pattern**
- **Deduce f**
- Rewrite for f^{-1}

COLLABORA

TECHNIQUES

Waiting

- Cuss on IRC.
- Wait for a draconequus to whisper *f* to you.

Works 20% of the time

Law of Parsimaney

- Simple *f* are more likely than complex *f*.
- Simple for the *hardware*, not for you!
- Think like a hardware designer (gate count).

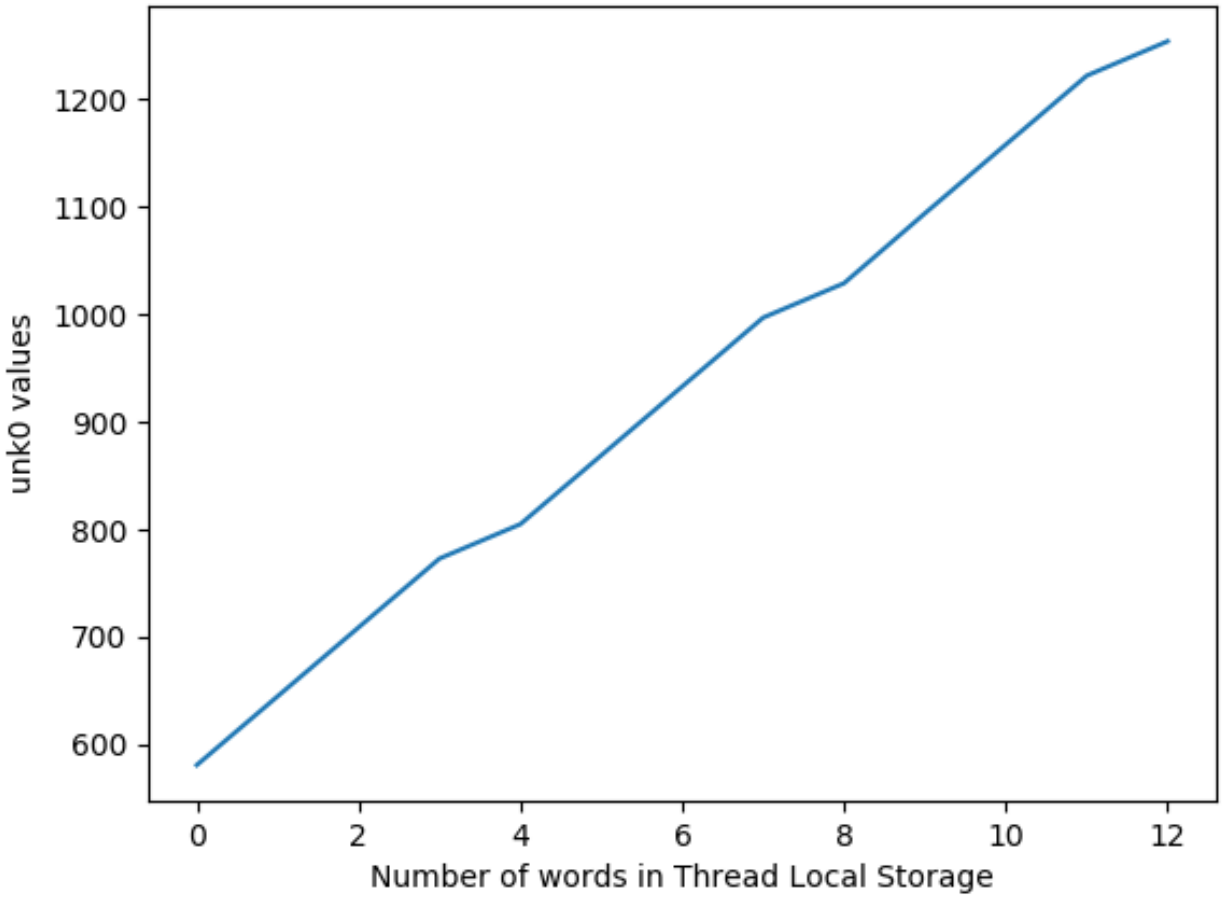
Properties

- Alignment?
- Monotonicity?
- Linear? *Almost* linear?
- Bitwise complements?
- Powers of two?

Information entropy

- Input entropy vs output bit count
- Equal entropy: just shuffling
- More in input: incomplete encoding (pigeonhole)
- More in output: incomplete input (Occam's Razor)

Graphs


1200
1100
1000
900
800
700
600
unk0 values
0
2
4
6
8
10
12
Number of words in Thread Local Storage

Calculus

- Discrete derivatives (backwards differencing)
- Sometimes modeling *f'* is easier than *f*.
- Integrate *f'* to recover *f* (summation)

Useful for near-linear f

Classes of *f*

- What kind of function could satisfy the properties?
- Closed-form algebraic?
- Bitwise manipulation?
- Try some.

Purpose

- Every field has a reason for being.
- Your job: figure out why.

Purpose

```
struct texture {
  unsigned width;
  unsigned unknown;
  unsigned depth;
  ...
```

Purpose

```
struct texture {
  unsigned width;
  unsigned height;
  unsigned depth;
  ...
```

Purpose

Proximate fields have proximate purposes.

Info drops

- Know the hardware, know the purpose.
- Conference slides.
- Vendor blogs.
- Code drops (kernel)
- Google is your friend.

XDC Hallway Track

[redacted]

If all else fails...

- Move on.
- Lots of seaponies in the sea.

COLLABORA

EXAMPLE

1

```
if (vColor.x < 0.5) discard;
```

```
flt r31.w, r0.x, #0.5
br.discard.true
```

2 - AND

```
if (vColor.x < 0.5 && vColor.y < 0.75)
    discard;
```

```
flt r31.w, r0.y, #0.75
flt r31.w, r0.x, #0.5
brx.discard.unk8888
```

2 - OR

```
if (vColor.x < 0.5 || vColor.y < 0.75)
    discard;
```

```
flt r31.w, r0.y, #0.75
flt r31.w, r0.x, #0.5
brx.discard.unkEEEE
```

2 - NAND

```
if (!(vColor.x < 0.5 && vColor.y < 0.75))
    discard;
```

```
flt r31.w, r0.y, #0.75
flt r31.w, r0.x, #0.5
brx.discard.unk1111
```

2 - NOR

```
if (!(vColor.x < 0.5 || vColor.y < 0.75))
    discard;
```

```
flt r31.w, r0.y, #0.75
flt r31.w, r0.x, #0.5
brx.discard.unk7777
```

Expression	Code
(A && B)	8888
(A || B)	EEEE
!(A && B)	7777
!(A || B)	1111

3?

```
if (vColor.x < 0.5 && vColor.y < 0.75 &&
    vColor.z == 1.0) discard;
```

```
flt r31.x, r0.y, #0.75
feq r31.w, r0.z, #1
flt r31.w, r0.x, #0.5
brx.discard.unk8080
```

4?

```
if (vColor.x < 0.5 && vColor.y < 0.75 &&
    vColor.z == 1.0 && vColor.w == 0.0)
        discard;

feq r31.w, r0.z, #1
feq r31.w, r0.w, #0
flt r31.x, r0.y, #0.75
flt r31.w, r0.x, #0.5
brx.discard.unk8000
```

5?

```
if (vColor.x < 0.5 && vColor.y < 0.75 &&
    vColor.z == 1.0 && vColor.w == 0.0 &&
    vColor.x > vColor.y) discard;
```

```
...
iand r31.w, r0.z, r0.w
brx.discard.unk8000
```

Expression	Code
(A && B)	8888
(A || B)	EEEE
!(A && B)	7777
!(A || B)	1111
(A && B) && C	8080
(A && B) && C && D	8000

Mathemagics

$$f(x_1, x_2, x_3, x_4) = y$$

Expression	Code
(A && B)	8888
(A || B)	EEEE
!(A && B)	7777
!(A || B)	1111
(A && B) && C	8080
(A && B) && C && D	8000

Expression	Code
(A && B)	8888
!(A && B)	7777
(A || B)	EEEE
!(A || B)	1111

Expression	Code	
(A && B)	8888	FFFF
!(A && B)	7777	
(A || B)	EEEE	FFFF
!(A || B)	1111	

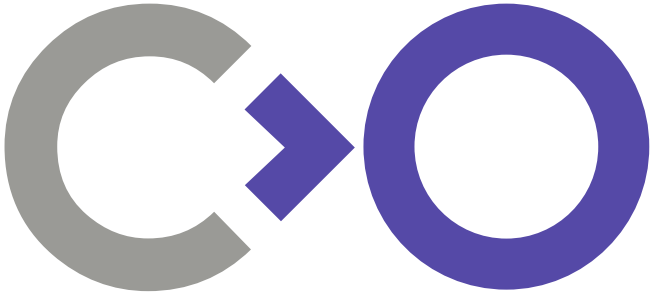
Expression	Code
(A && B) && C && D	8000

0	0
0	0
0	0
0	0
0	0
.	.
.	.
.	.
0	0
0	0
1	1

Expression	Code
(A && B)	8888
(A || B)	EEEE
!(A && B)	7777
!(A || B)	1111
(A && B) && C	8080
(A && B) && C && D	8000

COLLABORA

LUT



Thank you!

COLLABORA

TOP SECRET

CONFIDENTIAL