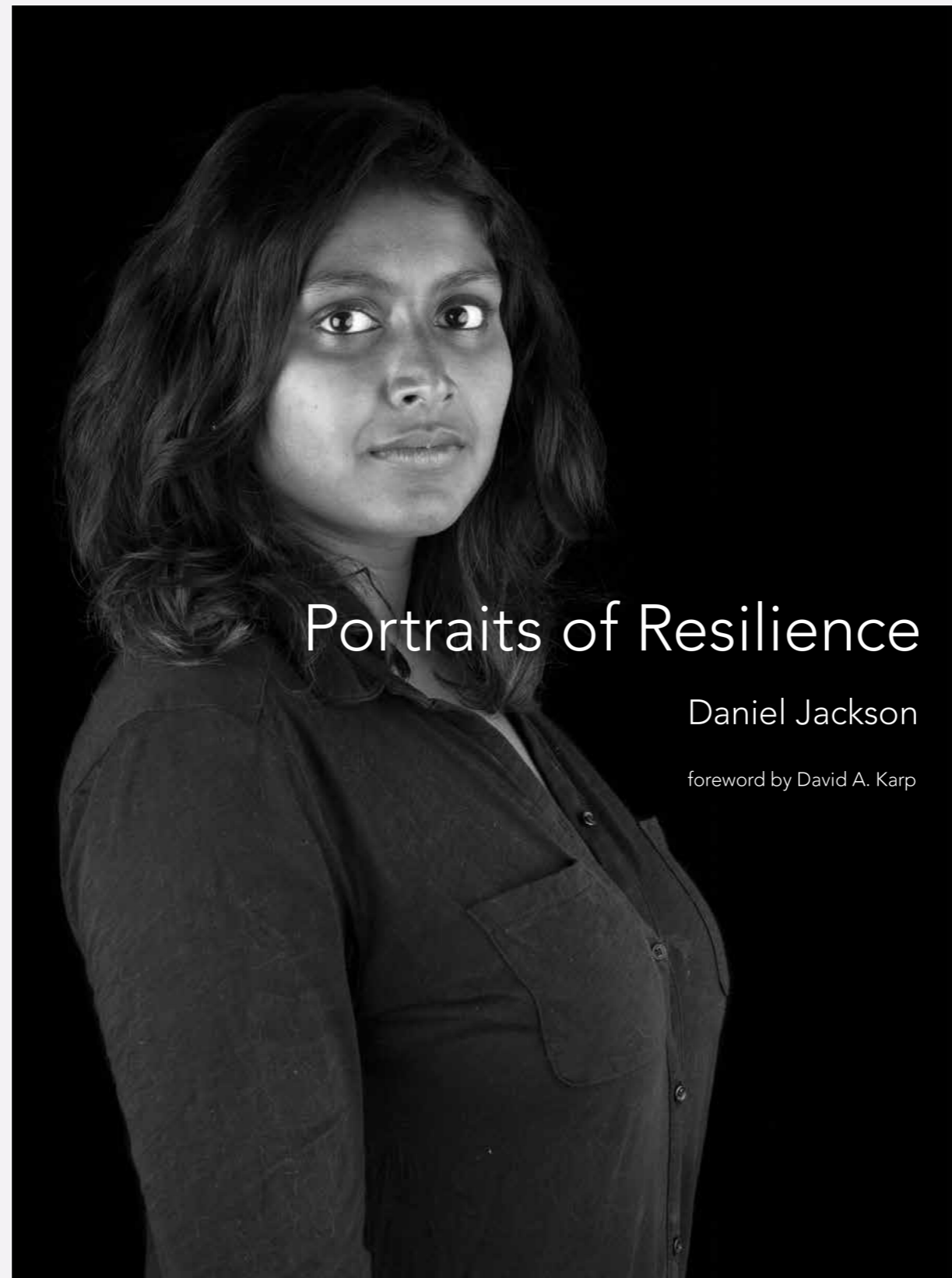


a new way to  
think about  
specifications

**Daniel Jackson · CSAIL, MIT**

ABZ · June 7, 2018

# a different project



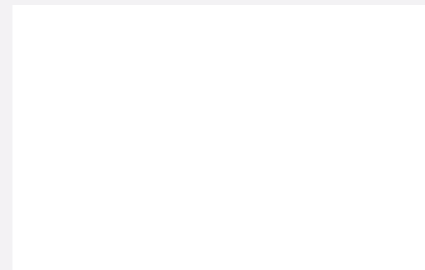
<http://portraitsofresilience.com>

how bugs  
led us astray

# the software problem



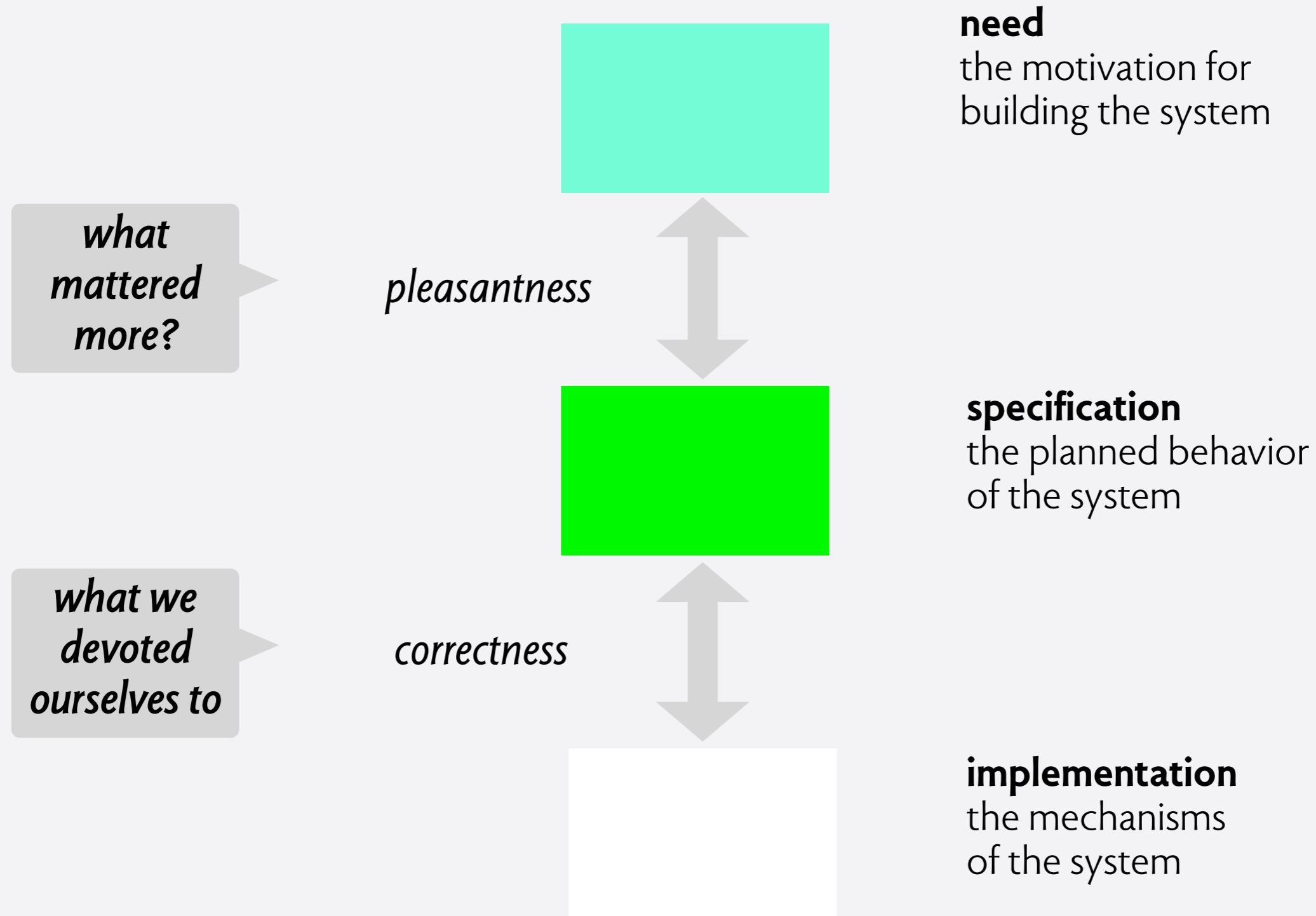
**need**  
the motivation for  
building the system



**implementation**  
the mechanisms  
of the system



# separating concerns



# correct $\Rightarrow$ useful ?

Primary Social Promotions +

☆ me, Alyssa (12) hacking meetups javascript - Hello again Be 11:48 am

label:hacking

☆ me, Alyssa (12) Inbox meetups javascript - Hello again Ben 9:43 am

label:meetups

☆ me, Alyssa (12) Inbox hacking javascript - Hello again Ben. 9:58 am

label:hacking label:meetups

☆ me, Alyssa (12) Inbox hacking javascript - Hello again Ben. 9:58 am

🔍 No messages matched your search. Try using [search options](#) such as sender, date, size and more.

# correct $\Rightarrow$ useful ?

correctness & pleasantness  
are not independent

☐ ▾ ↻ More ▾ 1-2 of 2 < > 🗃️ ▾ ⚙️ ▾

[Empty Trash now](#) (messages that have been in Trash more than 30 days will be automatically deleted)

☐	🗑️	me, Alyssa (13)	hacking	meetups	todo	javascript - Hello a	11:48 am
☐	🗑️	<b>Andy from Google</b>	Updates	<b>Ben, welcome to your new Googl</b>			9:01 am

label:todo ▾ 🔍 🗃️ 🔔 B

☐ ▾ ↻ More ▾ 🗃️ ▾ ⚙️ ▾

There are no conversations with this label.

label:todo label:trash ▾ 🔍 🗃️ 🔔 B

☐ ▾ ↻ More ▾ 1-1 of 1 < > 🗃️ ▾ ⚙️ ▾

☐	🗑️	me, Alyssa	Trash	hacking	meetups	todo	javascript -	10:11 am
---	----	------------	-------	---------	---------	------	--------------	----------

label:todo OR label:meetup ▾ 🔍 🗃️ 🔔 B

☐ ▾ ↻ More ▾ 🗃️ ▾ ⚙️ ▾

🔍 Some messages in Trash or Spam match your search. [View messages.](#)

# correct $\Rightarrow$ useful ?

This screenshot shows the Gmail search interface. The search bar contains the query 'in:sent'. The search results show one email with the subject 'javascript - Yes, it does. On' and the recipient 'Alyssa P. Hacker (2)'. The email is currently in the 'Inbox' and 'hacking' categories. The interface includes a 'COMPOSE' button, a sidebar with 'Inbox', 'Starred', and 'Sent Mail', and a top navigation bar with the Google logo and user profile 'B'.

This screenshot shows the details of the email selected in the previous view. The subject is 'javascript' and it is categorized under 'Inbox' and 'hacking'. The email is from 'Alyssa P. Hacker' with the subject 'Reminds you of the old days, eh?' and is dated '9:14 PM (33 minutes ago)'. A second email from 'Ben Bitdiddle' is visible below, dated '9:40 PM (7 minutes ago)', with the subject 'Yes, it does.' and the recipient 'to Alyssa'. The interface includes a 'COMPOSE' button, a sidebar with 'Inbox', 'Starred', 'Sent Mail', 'Drafts', 'Trash', and 'Categories', and a top navigation bar with the Google logo and user profile 'B'.

# correct $\Rightarrow$ safe ?

airborne  $\Leftrightarrow \neg$ WheelPulse

**environment**

$\neg$ WheelPulse  $\Leftrightarrow$  disabled

**specification**

airborne  $\Leftrightarrow$  disabled

**requirement**

$\wedge$

$\Rightarrow?$



Airbus A320, Warsaw 1993

# correct $\Rightarrow$ secure ?

From: "TIG" <[help@MIT.EDU](mailto:help@MIT.EDU)>  
Date: October 13, 2008 11:04:08 AM EDT  
To: "'Daniel Jackson'" <[dnj@csail.mit.edu](mailto:dnj@csail.mit.edu)>  
Subject: your password

We recently ran a password checker to evaluate passwords of all CSAIL users, and your password was readily broken. Please choose a new password ASAP...

my password:

sergeantpepper1967

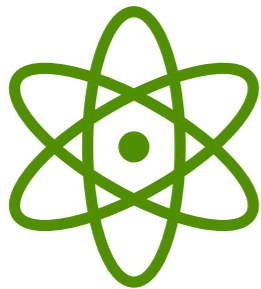
8 char limit: passwd utility silently truncated rest

*Aydal [2009]*

*Analyzed Tokener for security  
Found 9 anomalous scenarios  
eg, new configuration file silently  
ignored if one exists on disk*

# a research program

explore software design  
what makes a good spec



a design theory



design case studies



design patterns

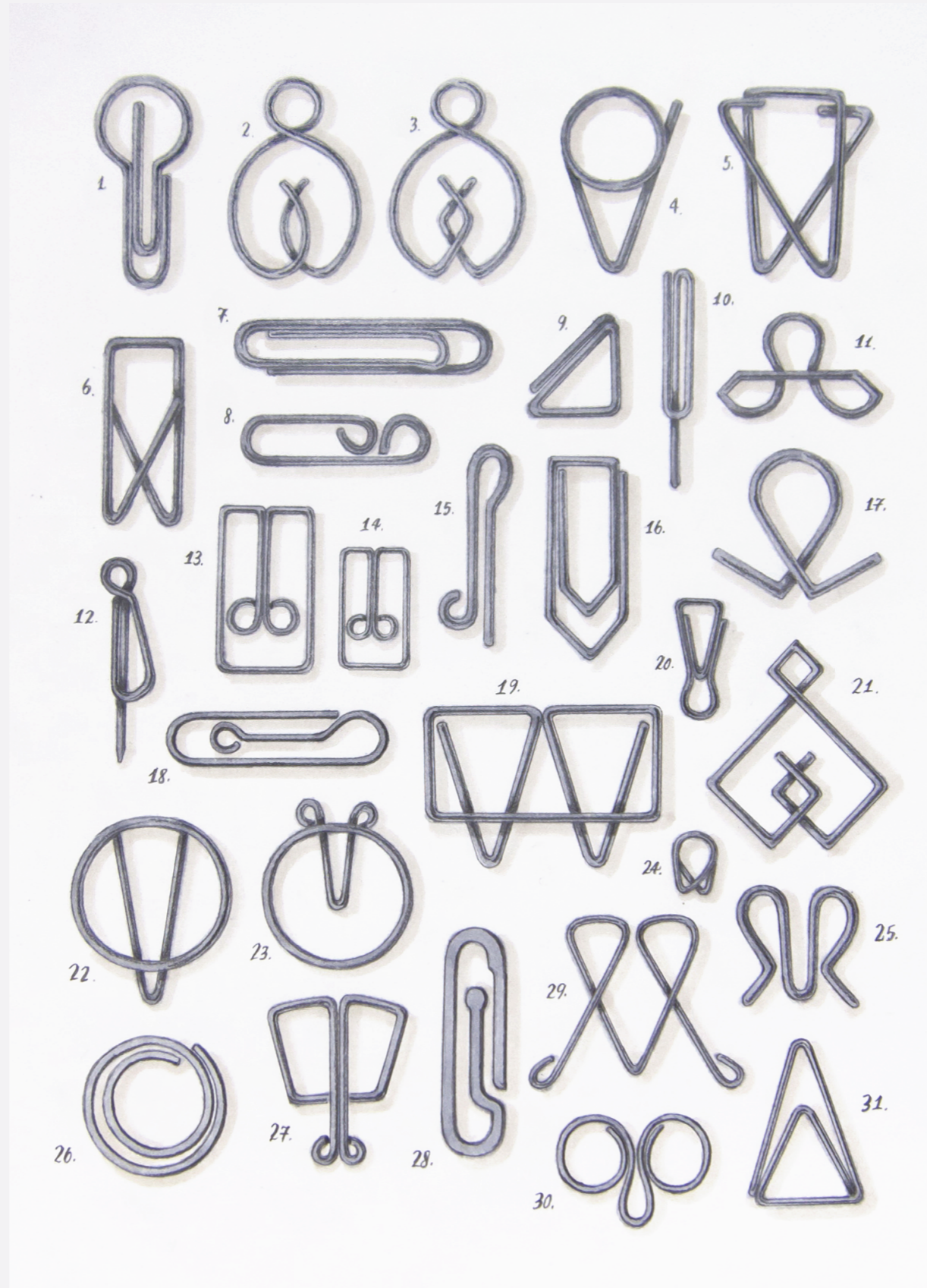


code platform

how is  
design  
done?



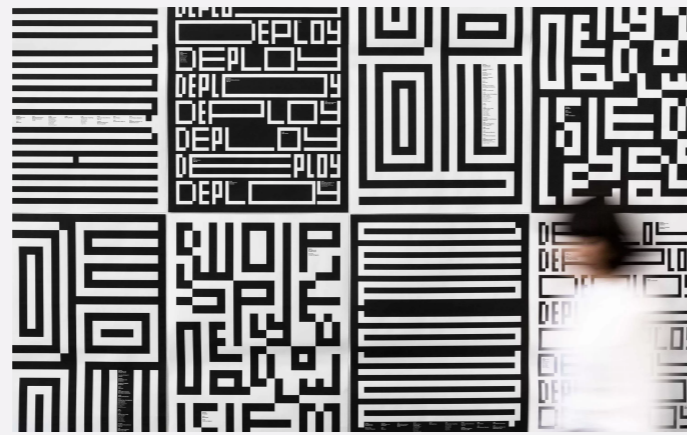
# simple design



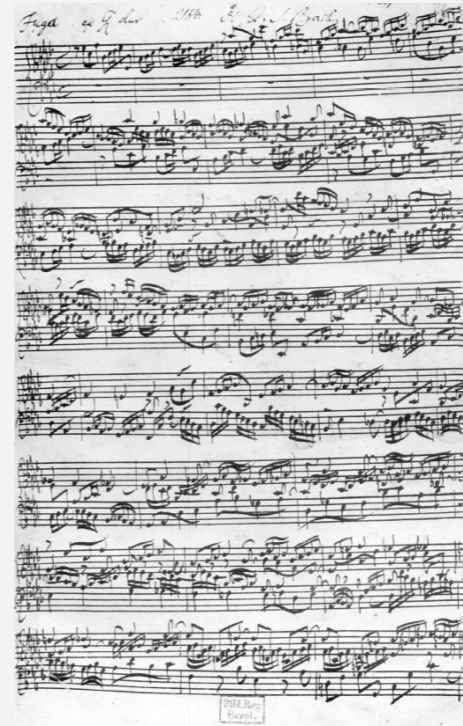
# complicated design



architecture



graphic design



music



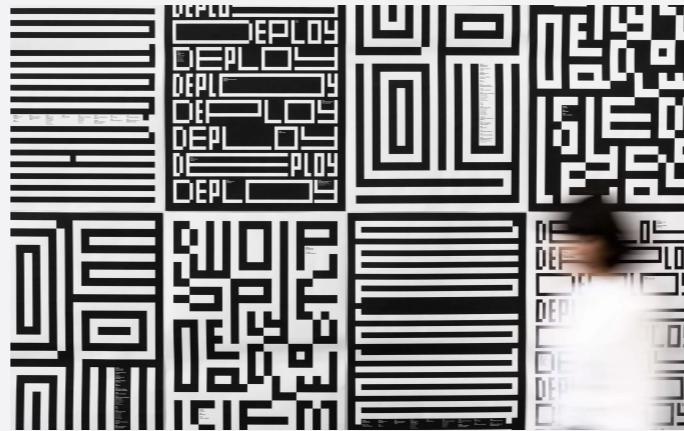
software



# core concepts: a universal design strategy



architecture



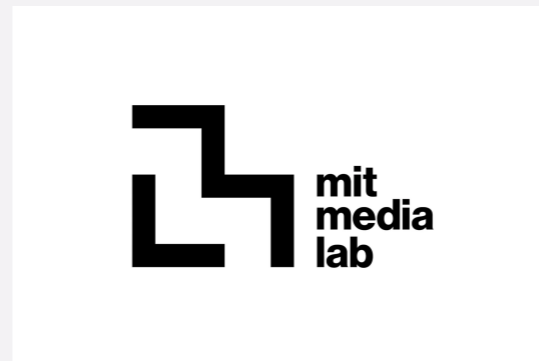
graphic design



music



massing



identity



motif

# core concepts for software



core concepts:  
**song, playlist**



core concepts:  
**buffer**



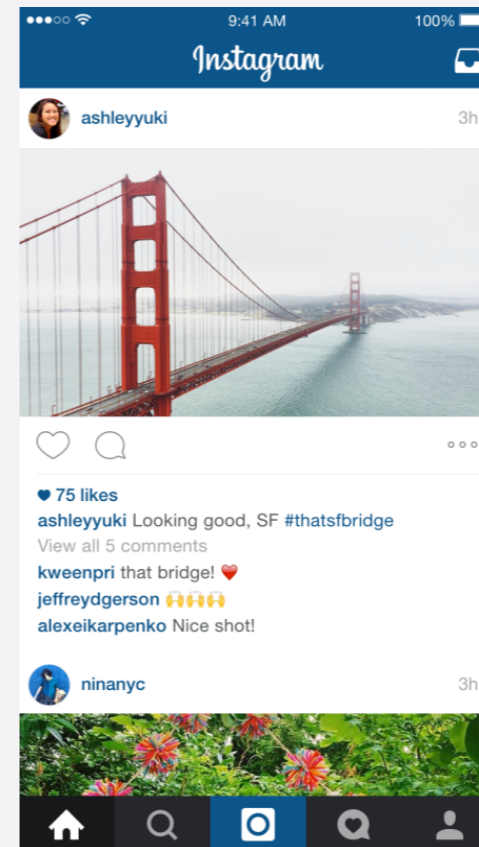
core concepts:  
**paragraph, styles**



core concepts:  
**paragraph, styles, linkedBox, page**



core concepts:  
**post, group, call**



core concepts:  
**photo, follow, like**



core concepts:  
**pixel map, layer/mask**



core concepts:  
**message, channel, mention**

concept  
basics

# what is a concept?



**inventive**

*so not just modeling*



**purposeful**

*so not an action*



**behavioral**

*so not an entity*



**self-contained**

*so not a feature or an abstract type*



**reusable**

*so not a feature*

## *trash*

## *reservation*



**inventive**

first in Apple Lisa (1982)  
not really about the GUI  
(despite Apple vs Msft, 1994)

for restaurants, started in 19th  
century (tables and rooms)



**purposeful**

purpose is:  
to undo deletions!

purpose is:  
efficient allocation  
of resources



**behavioral**

to delete a file, move to trash;  
can restore from there; to  
make space, empty trash

select resource to reserve;  
request reservation;  
make use of resource



**self-contained**

synergistic with file system  
but concept requires  
only set of objects

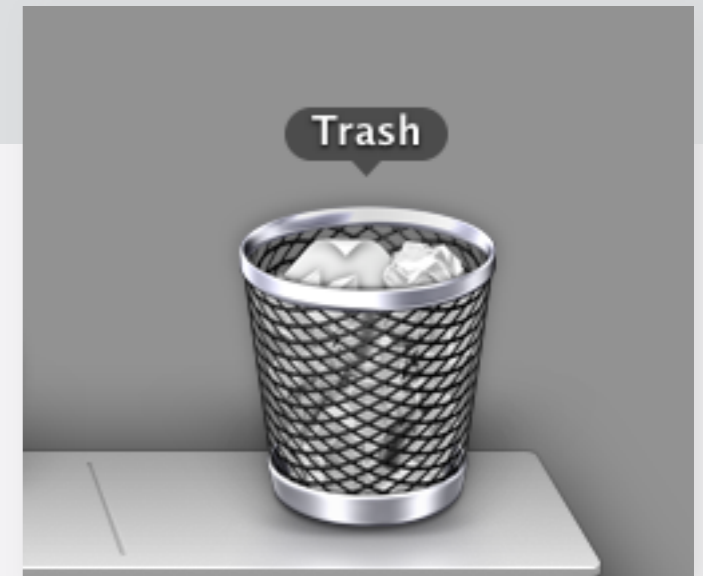


**reusable**

messages (Gmail)  
photos (iPhoto)  
posts (WordPress)  
notes (Evernote)

restaurant tables  
airplane seats  
medical appointments  
...

# the trash concept



purpose allow undo of deletion

**state** all, deleted: **set** X

**actions**

new (): X  $\hat{=}$  **result !in** all and all' = all + **result**

del (x: X)  $\hat{=}$  deleted' = deleted + x

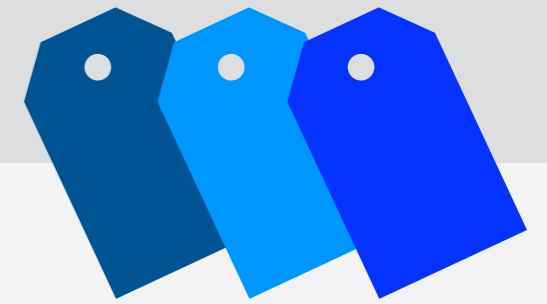
empty ()  $\hat{=}$  **no** deleted' **and** all' = all - deleted

spec showAll () : **set** X  $\hat{=}$  **result** = all

operational principle del(x) ... **not** empty() ... showAll():xs  $\Rightarrow$  x **in** xs  
del(x) ... empty() ... showAll():xs  $\Rightarrow$  x **not in** xs



# the label concept



purpose

organize items for  
easy retrieval

**state** labels:  $X \rightarrow \text{Label}$

**actions**

mark ( $x: X, p: \text{Label}$ )  $\triangleq$  labels' = labels +  $x \rightarrow p$

unmark ( $x: X, p: \text{Label}$ )  $\triangleq$  labels' = labels -  $x \rightarrow p$

find ( $ps: \text{set Label}$ ): **set**  $X \triangleq$  **result** = { $x \mid ps \text{ in } x.\text{labels}$ }

spec

show ( $x: X$ ): **set**  $\text{Label} \triangleq$  **result** =  $x.\text{labels}$

operational principle

mark( $x,p$ ) ... **not** unmark( $x,p$ ) ... search( $p$ ): $xs \Rightarrow x \text{ in } xs$

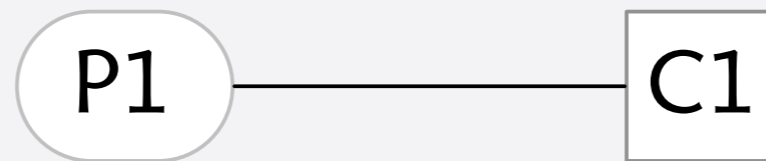
**not** mark( $x,p$ ) ... search( $p$ ): $xs \Rightarrow x \text{ not in } xs$

the  
singularity  
rule

# one-to-one mapping

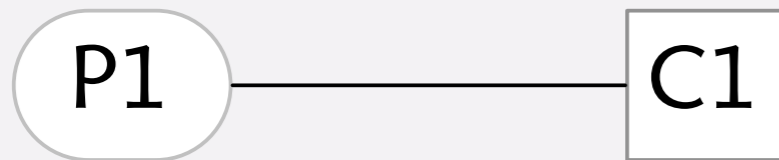
*purposes*

*concepts*

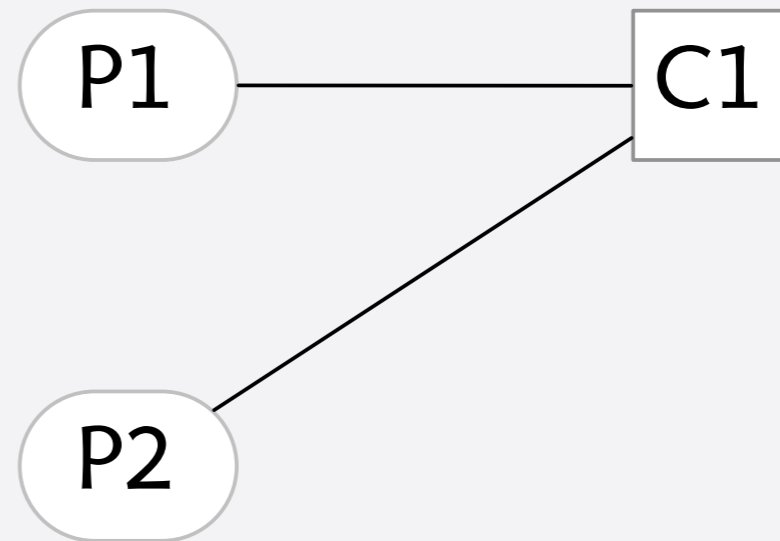


# four ways to fail

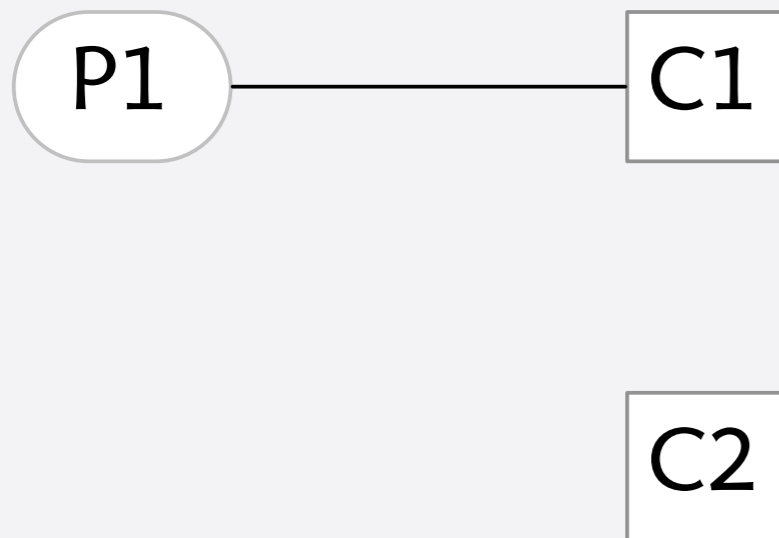
unfulfilled purpose



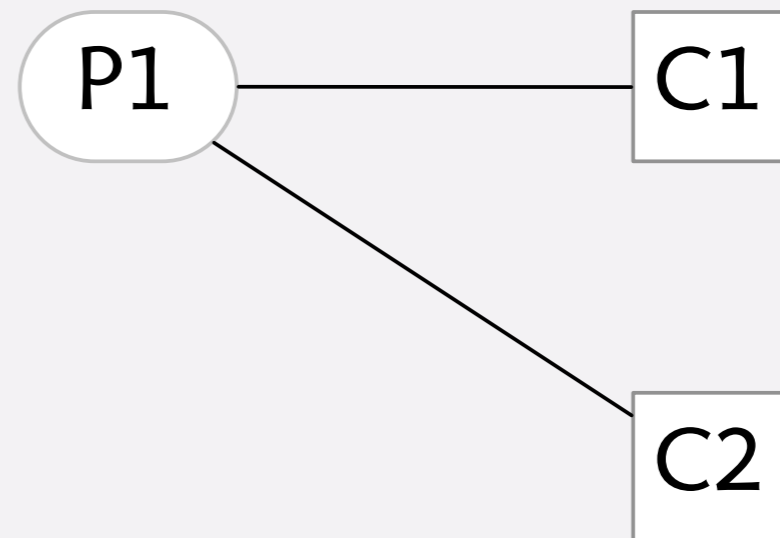
overloaded concept



unmotivated concept



redundant concepts



# my camera fuji x100s



# image quality setting





# aspect ratio



# image size setting





# non-standard ratio + raw?



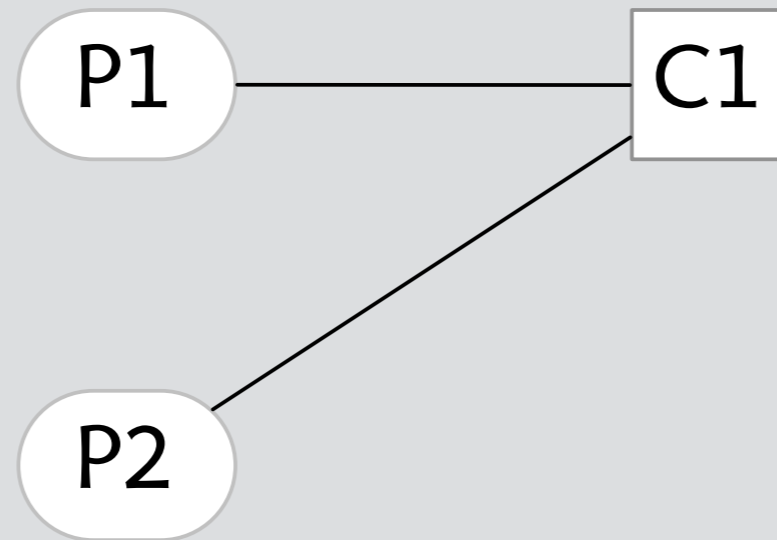
# what you can't do

non-standard aspect ratio + raw  
even though raw images get nice nondestructive crop!



# overloaded concepts

No one can serve two masters. Either you will hate the one and love the other, or you will be devoted to the one and despise the other. [Matthew 6:24]



4 forms of overloading:

**piggybacking** new purpose hacked onto old concept

**false convergence** two purposes looked the same

**emergent purpose** second purpose emerged with use

**denial** designer believes second purpose unnecessary



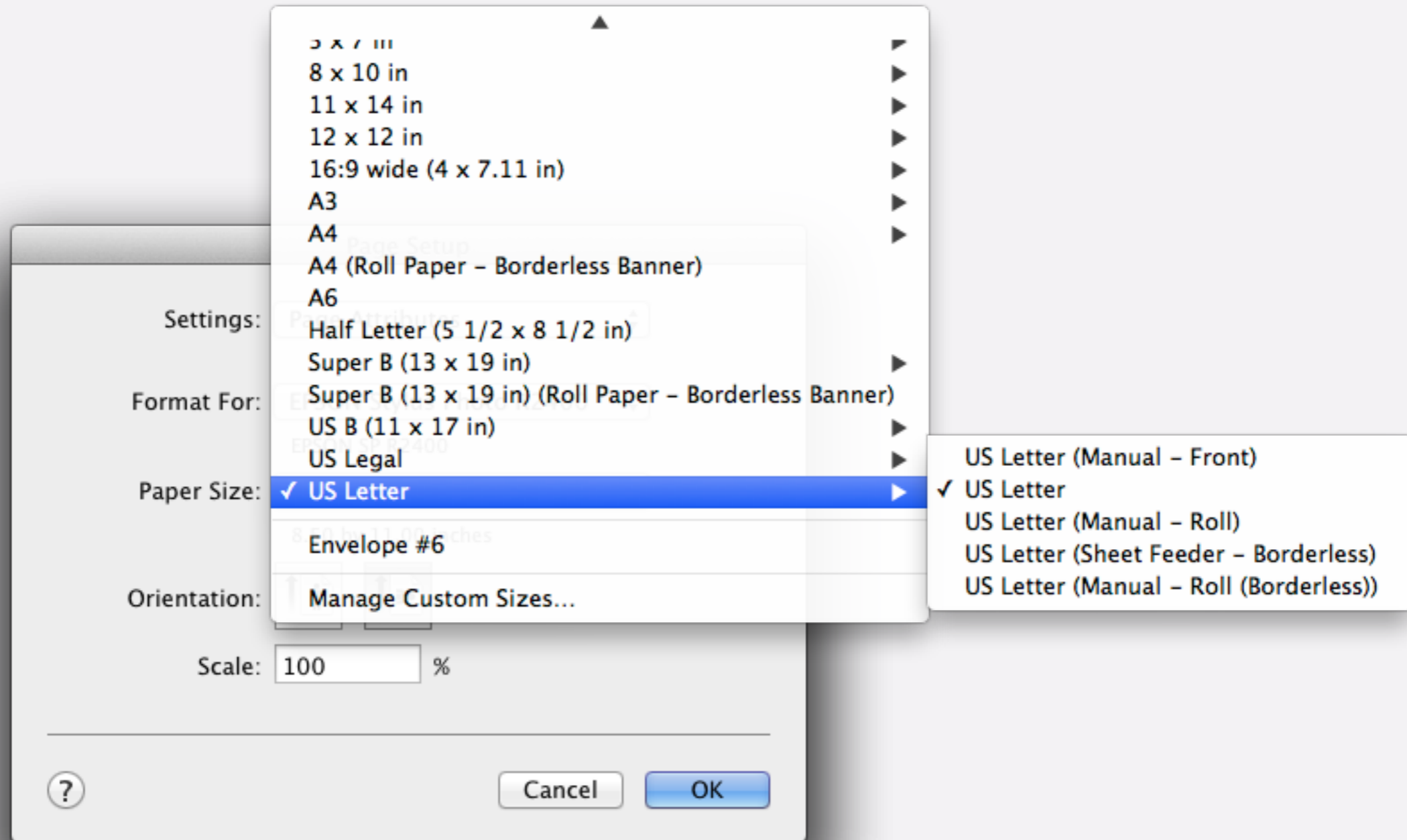
# piggybacking fuji camera

new purpose hacked onto old concept

L	3:2	664
L	16:9	681
L	1:1	702
M	3:2	707
M	16:9	719
M	1:1	734
S	3:2	746

image size  
aspect ratio piggybacked  
on JPEG dimensions

# piggybacking Epson driver



result: can't create custom size for front loading  
also, page size presets in Lightroom hold feed setting

# false convergence facebook friend

two purposes looked the same



filter incoming posts  
control access to my posts  
**distinct purposes**

2011: Facebook added  
subscribe/follow

# emergent purpose email subject

users find second purpose for concept

To: Daniel Jackson <dnj@mit.edu>

Re: Catch me if you can in real life!

initial purpose: summarize content

To: csail-related@lists.csail.mit.edu

Re: [csail-related] turn off the lights?

**emergent purpose: show sender**  
if you bcc a list, subject reveals to-address

thanks to Shriram Krishnamurthi

To: Daniel Jackson <dnj@mit.edu>

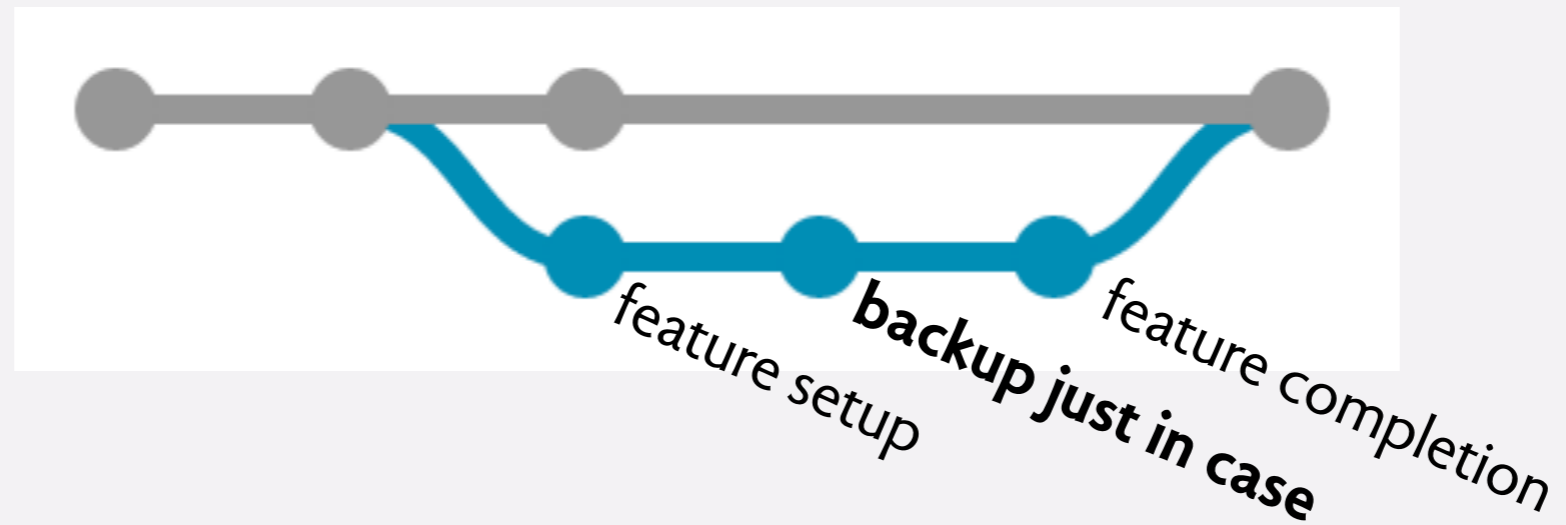
your trip reservation

**emergent purpose: group by conversation**  
can't label reservations from Expedia by trip

thanks to Eunsuk Kang

# denial commit

designer believes second purpose unnecessary

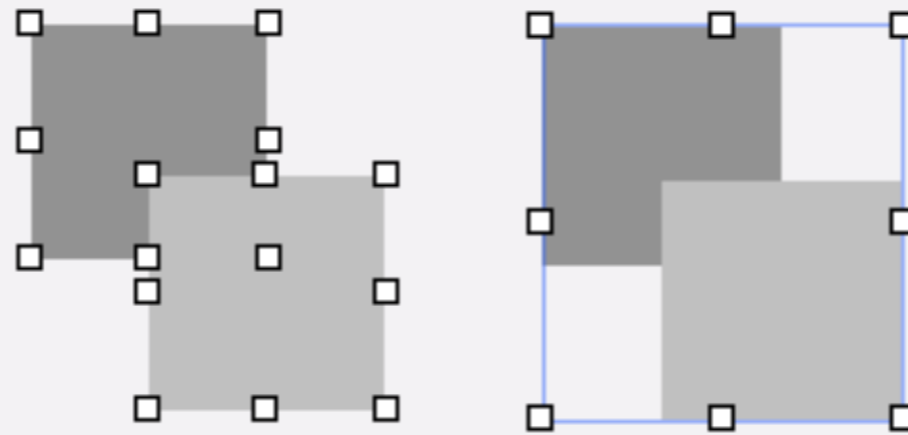




the  
uniformity  
rule

# what makes a usable concept?

operational principle is uniform  
always the same actions, irrespective of context



*concept:* **Group** (Keynote)

*purpose:* treat set as one

*OP:* ... select(objs); group(); mutate()

quantified over state & args

**unless** objs contains a text body object

# non-uniformity range

concept: **Range** (Numbers)

purpose: define formula over adjustable group of cells

OP: ... define(f, c, R) ... new(rc, dir): nc ... enter(nc,v) ... show(c)

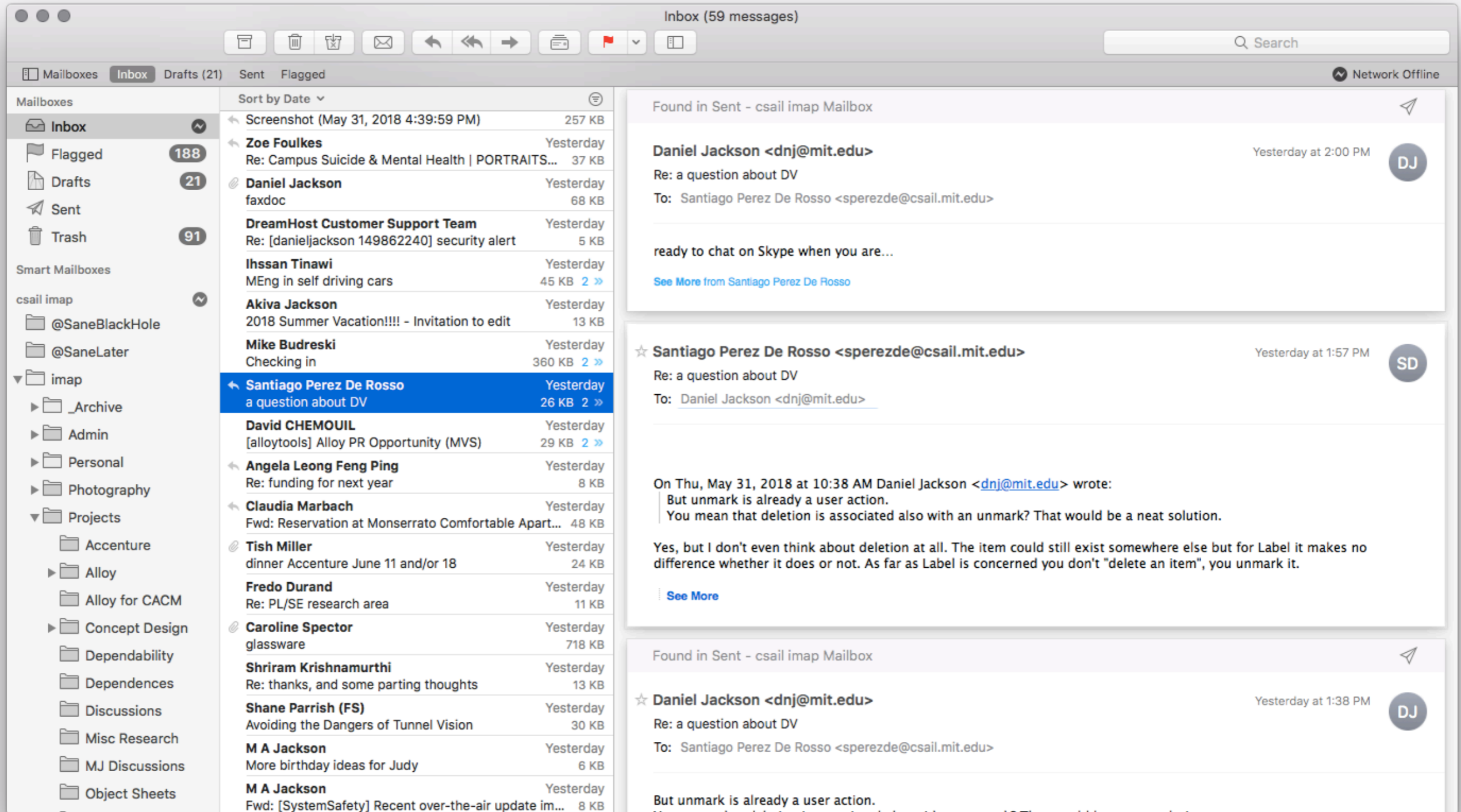
**unless** range cell rc is at top of range and dir is above or...

	A	B
1	item	cost
2	apples	\$4
3	bananas	\$2
4	grapes	\$6
5	kiwis	\$3
6		
7		

• fx SUM B2:B5

	A	B
1	item	cost
2	apples	\$4
3	bananas	\$2
4	cherries	
5	grapes	\$6
6	kiwis	\$3
7		
8		\$15

# non-uniformity conversation



action applied to every message in conversation **unless** message in other folder or action is reply ...

# kinds of non-uniformity

*varies  
over type*

Keynote grouping **unless** objs contains a text body object

*varies over  
mode*

Fuji aspect ratio setting **unless** set to raw only mode

*varies  
over state*

Dropbox share folder **unless** folder is ancestor or descendant of shared folder

*varies  
over state*

Git branch **unless** working directory contains uncommitted file or...

*varies  
over arg*

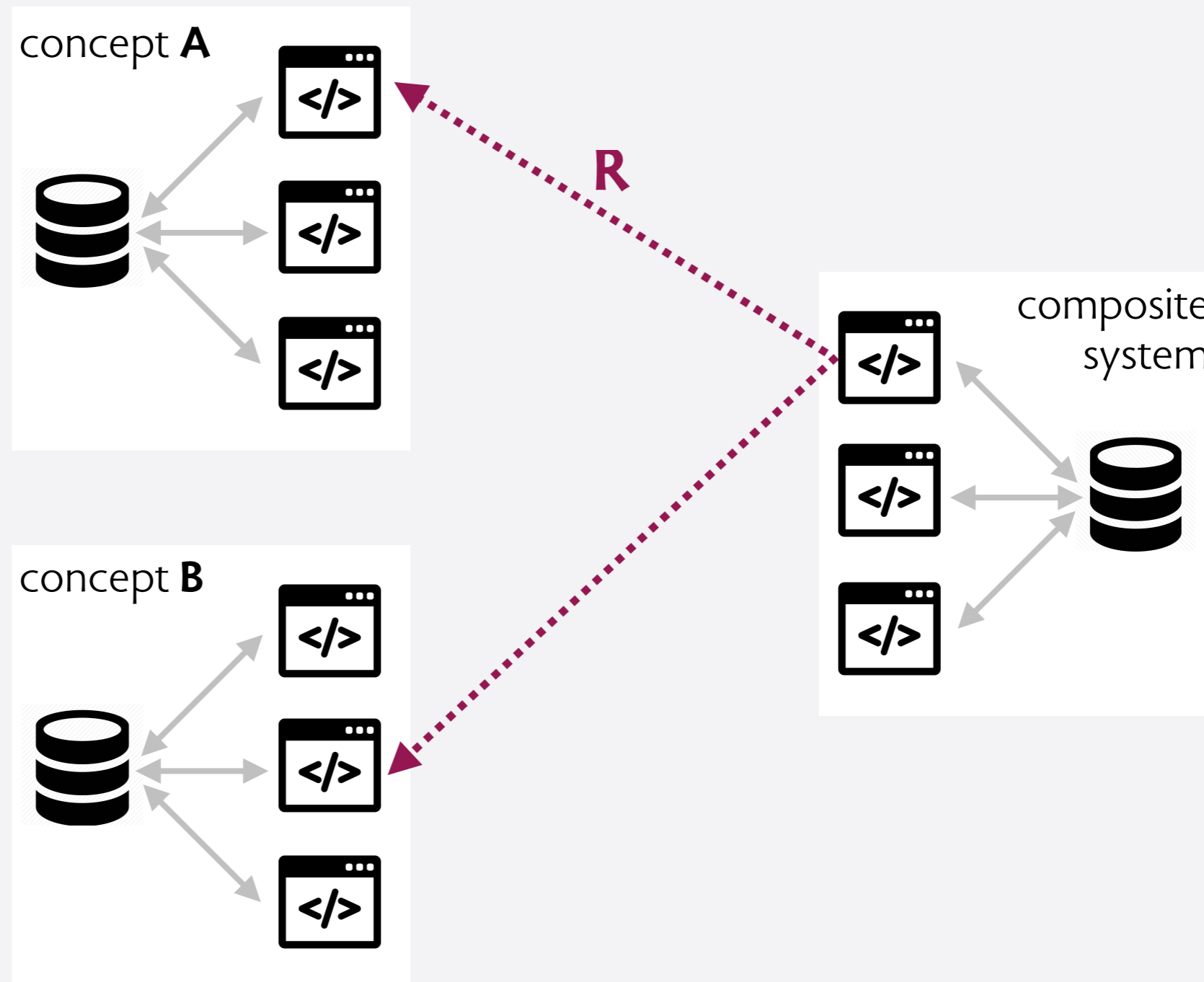
Twitter mention **unless** mention includes first character of tweet



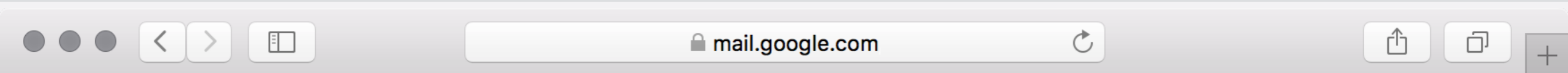
the  
integrity  
rule

# interpreting composite behavior

each action in composite system  
interpreted as zero or more actions in each concept



# example gmail



in:sent

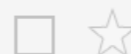


Gmail



More

1-1 of 1



To: Alyssa P. Hacker (2)

Inbox

hacking

javascript - Yes, it does. On

9:40 pm

COMPOSE

Inbox

Starred

Sent Mail

Drafts

Trash

Categories

Social

Promotions

Updates

Forums

hacking

meetups

todo

More

0 GB (0%) of 15 GB used  
[Manage](#)

[Terms](#) - [Privacy](#)

Last account activity: 26 minutes ago  
[Details](#)

action is **Label.show**( $p$ ): $ms$   
where  $p$  is the label *sent*  
and  $ms$  is the set of two messages listed

prior sending of msg  $m$  was an instance of  
action **Label.mark**( $m$ ,  $p$ )  
where  $p$  is the label *sent*

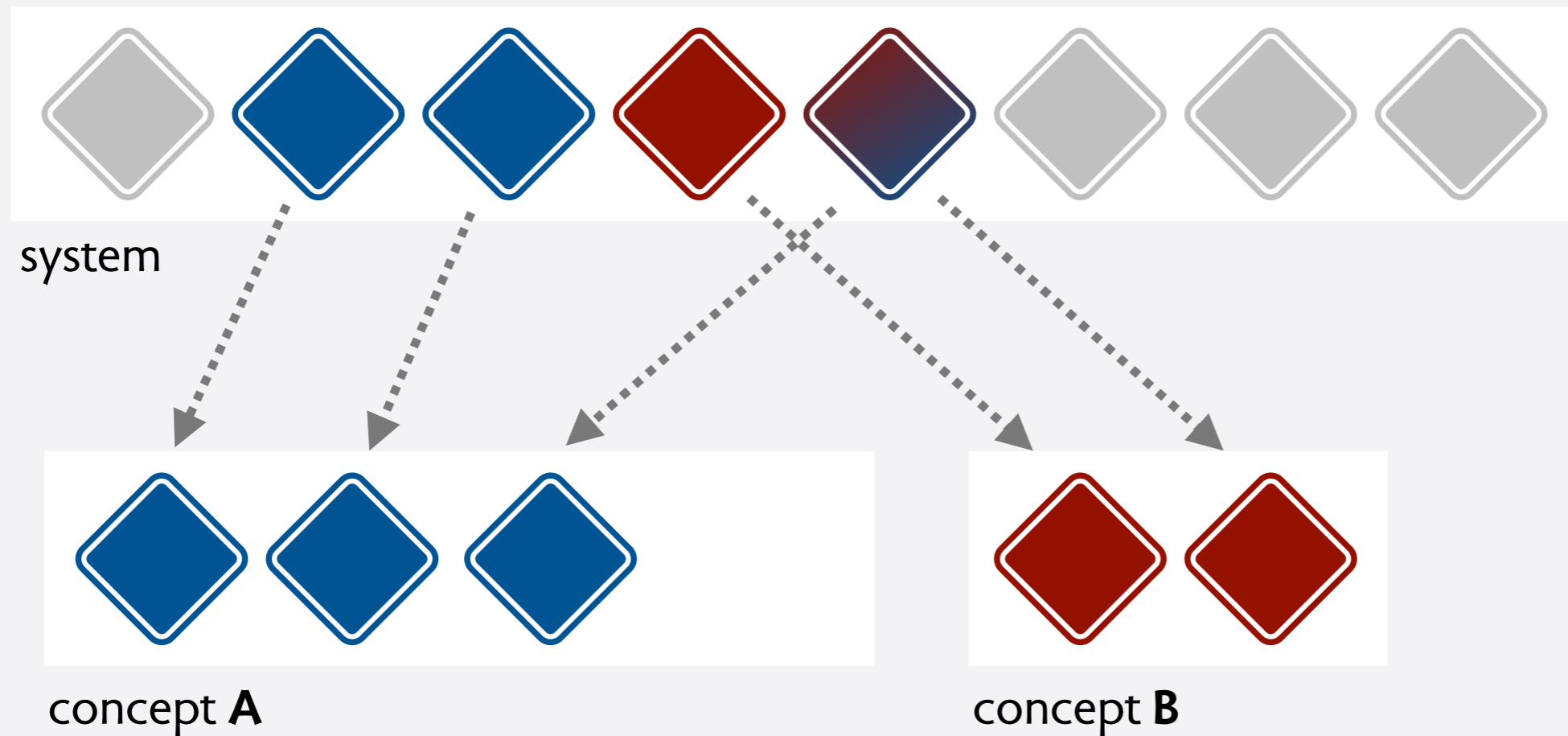


# judging composite behavior

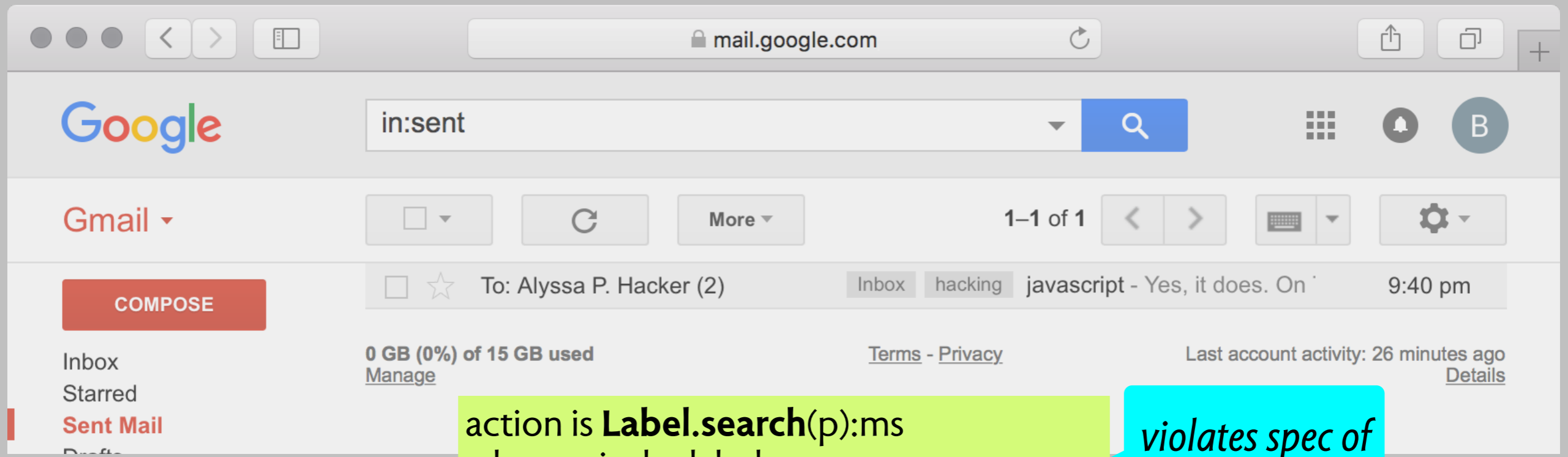
a simple criterion

projected behavior must satisfy concept spec:

$$\forall c: \text{concept} \mid \forall t: \text{traces}(\text{sys}) \mid R_c(t) \in \text{traces}(c)$$

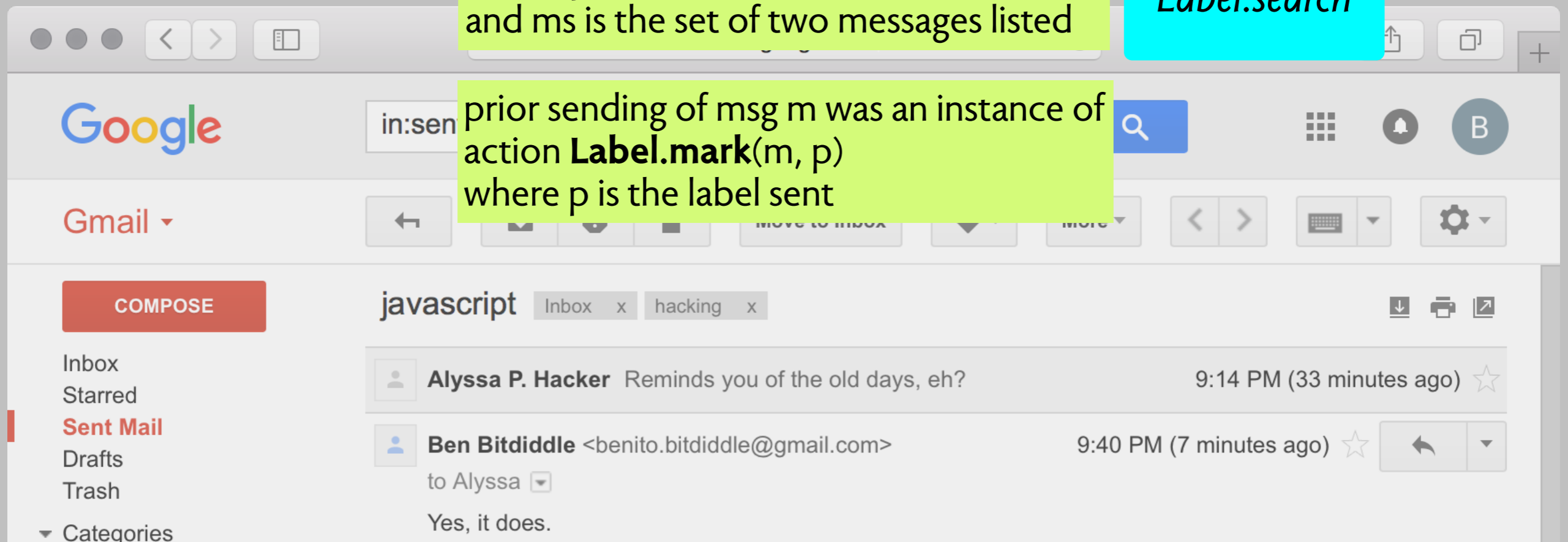


# example gmail



action is **Label.search(p):ms**  
where p is the label sent  
and ms is the set of two messages listed

*violates spec of  
Label.search*



prior sending of msg m was an instance of  
action **Label.mark(m, p)**  
where p is the label sent



# integrity violations trash



interaction of Trash and Volume (Apple Finder)  
unmount of Volume removes files from Trash  
not expressible in terms of Trash actions  
a solution: one trash/volume

# integrating concepts to make apps

Deja Vu (Santiago Perez De Rosso)


library of polymorphic concepts, each implementing full stack composed in HTML by linking actions

app	Authentication	Authorization	Passkey	Market	Rating	Follow	Geolocation	Post	Comment	Event	Label	Group	Task	Checklist	Property	Scoring	Chat
Accord	1	1	0	0	1	0	0	0	0	0	0	1	0	2	2	1	0
ChoreStar	2	2	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0
MapMIT	1	1	0	0	0	0	2	0	0	1	0	1	0	0	1	0	0
Rendezvous	1	1	0	0	0	0	2	1	1	1	1	1	0	0	1	0	0
SweetSpots	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1	0	0
Potluck	1	1	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0
GroceryShip	1	1	0	1	1	0	0	0	0	1	0	0	1	0	2	0	0
Lingua	1	1	0	0	0	0	0	0	1	0	1	0	0	0	1	1	1
LiveScorecard	1	1	2	0	0	0	0	0	0	1	1	2	1	0	1	1	0

cliché

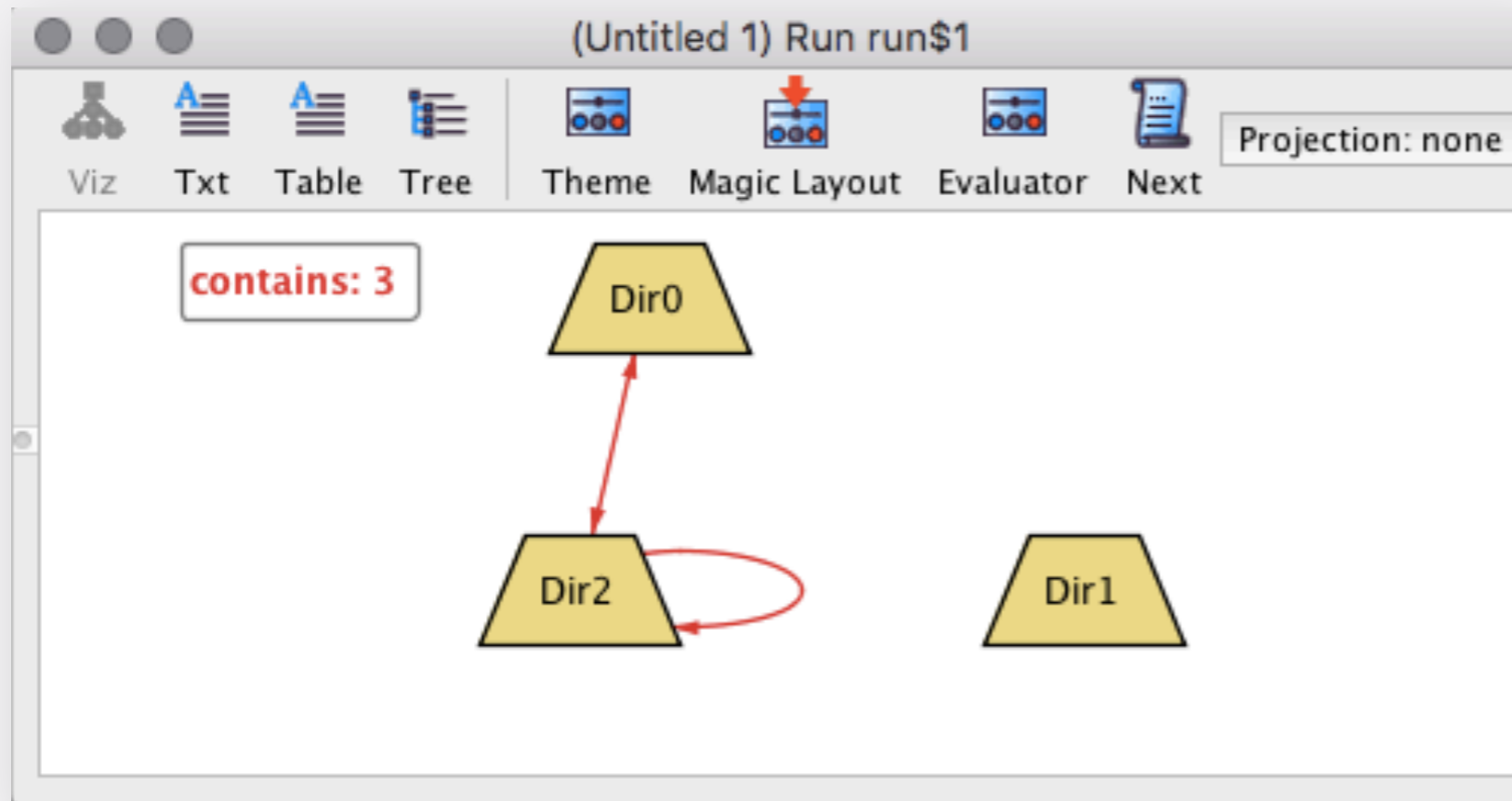
closing  
thoughts

# finding bugs in design: what kind?



```
sig Object {}  
sig File extends Object {}  
sig Dir extends Object {contains: set Object}  
run {}
```

mantras: to reduce costs, find bugs early  
**but what kinds of bugs?**  
corner cases easily found & fixed later  
snags vs snafus



*simulation > proof*

# models in design vs engineering

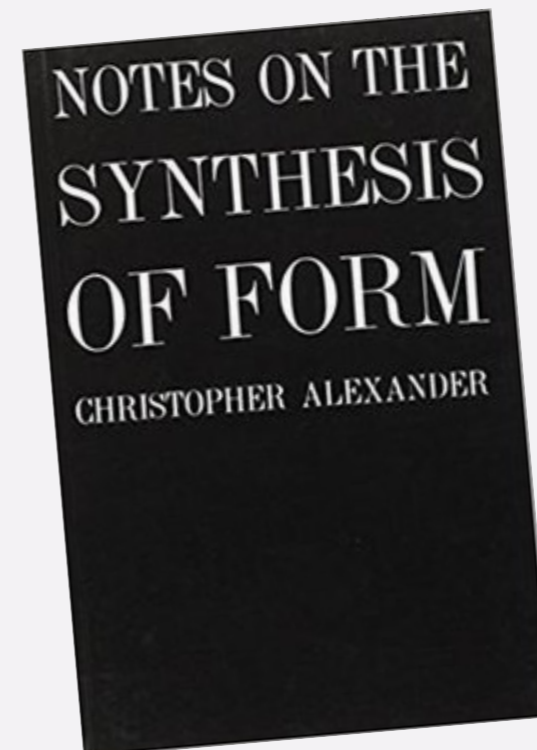
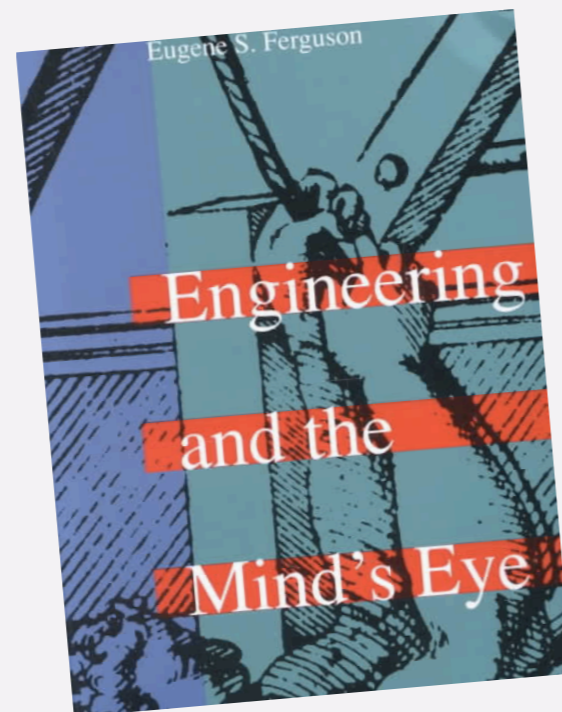
what engineers use models for?

calculating properties, checking against higher level specs  
to find bugs

*shallow flaws*

what designers actually use models for  
simulating experience of finished product  
to find unanticipatable misfits

*deep flaws*





## **the essence of UX design**

below surface of the UI, in the semantics

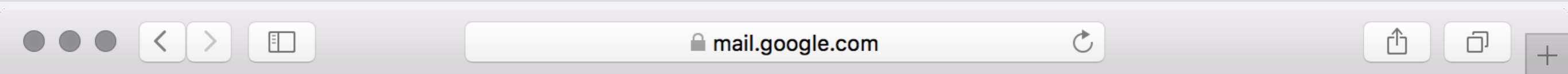
### **concepts: a structure for functionality**

purpose-driven & free standing

### **(de)constructing apps**

non-conflicting concepts are “conjunctive”

# organizing messages



label:hacking



Gmail ▾



More ▾

1-1 of 1



COMPOSE

- Inbox
- Starred
- Sent Mail
- Drafts
- Trash

▾ Categories

- Social
- Promotions
- Updates
- Forums

**hacking**

- meetups
- todo
- More ▾

Alyssa P. Hacker

Inbox

javascript - Reminds you of the old da

9:14 pm

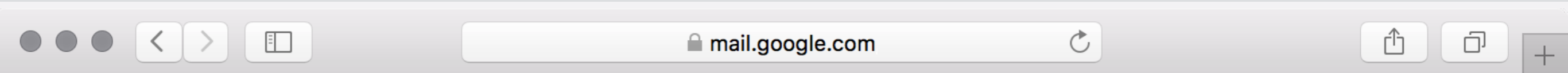
0 GB (0%) of 15 GB used  
[Manage](#)

[Terms](#) - [Privacy](#)

Last account activity: 14 hours ago  
[Details](#)



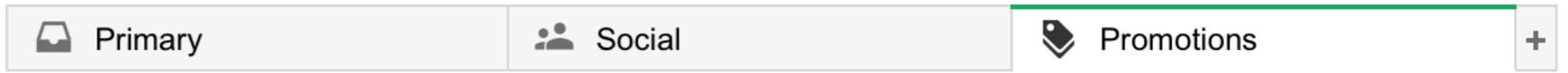
# automating filtering



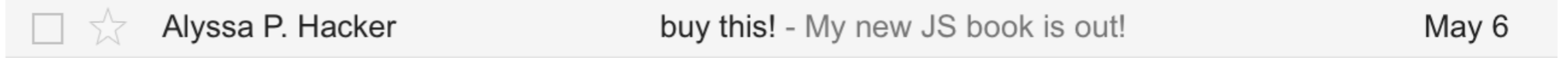
Gmail ▾



COMPOSE



**Inbox (2)**



- Starred
- Sent Mail
- Drafts
- Trash

0 GB (0%) of 15 GB used  
[Manage](#)

[Terms](#) - [Privacy](#)

Last account activity: 14 hours ago  
[Details](#)

Categories ▾

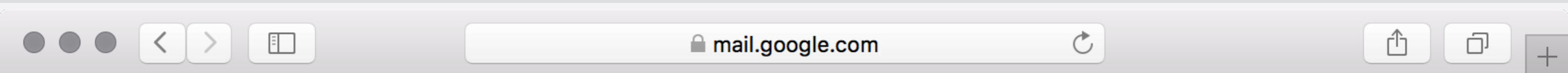
- Social
- Promotions
- Updates (1)**
- Forums

**hacking (1)**

- meetups
- todo
- More ▾



# slightly surprising behavior #1



in:sent



Gmail



Move to Inbox



More



COMPOSE

javascript

Inbox x hacking x



**Alyssa P. Hacker** Reminds you of the old days, eh? 9:14 PM (33 minutes ago)

**Ben Bitdiddle** <benito.bitdiddle@gmail.com> 9:40 PM (7 minutes ago)

to Alyssa

Yes, it does.



Click here to [Reply](#) or [Forward](#)

0 GB (0%) of 15 GB used  
[Manage](#)

[Terms](#) - [Privacy](#)

Last account activity: 26 minutes ago  
[Details](#)



# slightly surprising behavior #2

Primary Social Promotions +

☆ me, Alyssa (12) hacking meetups javascript - Hello again Be 11:48 am

label:hacking

☆ me, Alyssa (12) Inbox meetups javascript - Hello again Ben 9:43 am

label:meetups

☆ me, Alyssa (12) Inbox hacking javascript - Hello again Ben. 9:58 am

label:hacking label:meetups

No messages matched your search. Try using [search options](#) such as sender, date, size and more.



# slightly surprising behavior #3

Search bar: [ ] [Q] [Grid] [Bell] [B]

Actions: [ ] [Refresh] [More] 1-1 of 1 [Left] [Right] [Keyboard] [Settings]

Primary | Social | Promotions +

☆ me, Alyssa (10) [hacking] [meetups] javascript - Hello again Be 11:48 am

Search bar: has:nouserlabels [Q] [Grid] [Bell] [B]

Actions: [ ] [Download] [Warning] [Trash] [Move to Inbox] [Tag] [Refresh] [More] [Left] [Right] [Keyboard]

☆ Alyssa P. Hacker [Inbox] [Promotions] buy this! - My new JS box 10:33 am

☆ me, Alyssa (10) [Inbox] [hacking] [meetups] javascript - Oh, Al 9:24 am

# slightly surprising behavior #4

The image shows a sequence of four Gmail search results panels. The first panel shows a search for 'label:todo' which returns two messages: one from 'me, Alyssa (13)' with labels 'hacking', 'meetups', 'todo', and 'javascript - Hello a...', and another from 'Andy from Google' with a label 'Updates' and subject 'Ben, welcome to your new Googl'. The second panel shows the search 'label:todo' returning no results. The third panel shows the search 'label:todo label:trash' returning one message from 'me, Alyssa' with labels 'Trash', 'hacking', 'meetups', 'todo', and 'javascript -', dated '10:11 am'. The fourth panel shows the search 'label:todo OR label:meetup' returning no results, with a message in Trash or Spam matching the search.

1-2 of 2

[Empty Trash now](#) (messages that have been in Trash more than 30 days will be automatically deleted)

<input type="checkbox"/>		me, Alyssa (13)	hacking	meetups	todo	javascript - Hello a...	11:48 am
<input type="checkbox"/>		Andy from Google	Updates			Ben, welcome to your new Googl	9:01 am

label:todo

There are no conversations with this label.

label:todo label:trash

<input type="checkbox"/>		me, Alyssa	Trash	hacking	meetups	todo	javascript -	10:11 am
--------------------------	--	------------	-------	---------	---------	------	--------------	----------

label:todo OR label:meetup

Some messages in Trash or Spam match your search. [View messages.](#)

# slightly surprising behavior #5

The image shows a sequence of Gmail interface elements illustrating a search behavior. It starts with a message in the Promotions tab, then switches to the Social tab, and finally to a search for 'label:social label:promotions' which returns no results.

**Panel 1:** Gmail interface with tabs: Primary, Social, Promotions. Message from Alyssa P. Hacker: "buy this! - My new JS book is out" (10:33 am). The message is categorized as Promotions.

**Panel 2:** Gmail interface with tabs: Primary, Social, Promotions. Message from Alyssa P. Hacker: "buy this! - My new JS book is out!" (10:33 am). The message is categorized as Social.

**Panel 3:** Search bar contains "label:social".

**Panel 4:** Action bar with "Remove label" button. Message from Alyssa P. Hacker: "buy this! - My new JS book is out" (10:33 am). The message is categorized as Social.

**Panel 5:** Search bar contains "label:promotions".

**Panel 6:** Action bar with "Remove label" button. Message from Alyssa P. Hacker: "buy this! - My new JS book is out" (10:33 am). The message is categorized as Social.

**Panel 7:** Search bar contains "label:social label:promotions".

**Panel 8:** Action bar with "More" button.

**Panel 9:** Search results: "No messages matched your search. Try using [search options](#) such as sender, date, size and more."

## question

when you grow a design by adding a concept,  
how can you ensure its integrity is preserved?

## related question

given a design comprising some concepts,  
how can you tell if the concepts are mutually consistent?

## a really simple answer

1. interpret composite behavior in terms of concept actions
2. check that each behavior satisfies each concept's OP and spec

## notes

really saying: consistent if you can find an interpretation s.t. ...  
can attribute blame when one concept breaks another

# slightly surprising behavior #1

mail.google.com

Google

in:sent

Gmail

COMPOSE

Inbox

Starred

Sent Mail

Drafts

Trash

Categories

javascript

Inbox x hacking x

Alyssa P. Hacker Reminds you of the old days, eh? 9:14 PM (33 minutes ago)

Ben Bitdiddle <benito.bitdiddle@gmail.com> 9:40 PM (7 minutes ago)

to Alyssa

Yes, it does.

violates Label's operational principle:  
**not** mark(m,p) ... search(p):ms  $\Rightarrow$  m **not in** ms

attribute blame to Conversation

# slightly surprising behavior #2

The screenshot shows an email client interface. At the top, there are tabs for 'Primary', 'Social', and 'Promotions'. Below the tabs, a search bar contains the query 'label:hacking label:meetups'. To the right of the search bar are icons for a grid, a notification bell, and a profile icon 'B'. Below the search bar, there are buttons for 'More', a refresh icon, and a keyboard icon. At the bottom, a message states: 'No messages matched your search. Try using [search options](#) such as sender, date, size and more.'

violates nothing: expected behavior of Label and Conversation



# slightly surprising behavior #4

The screenshot shows the Gmail interface. At the top, there are navigation buttons: a checkbox with a dropdown, a refresh button, and a 'More' button. To the right, it says '1-2 of 2' with left and right arrow buttons, a keyboard icon, and a settings gear icon. Below this is a message list with two entries:

- me, Alyssa (13) with labels 'hacking', 'meetups', 'todo', and 'javascript - Hello a' at 11:48 am.
- Andy from Google with an 'Updates' label and subject 'Ben, welcome to your new Googl' at 9:01 am.

Below the message list is a search bar containing 'label:todo' and a search button. To the right of the search bar are icons for a grid, a notification bell, and a profile picture 'B'. Below the search bar is another set of navigation buttons: a checkbox with a dropdown, a refresh button, and a 'More' button. To the right, there is a keyboard icon and a settings gear icon. At the bottom, a message states: 'There are no conversations with this label.'

violates Label's operational principle:  
 $\text{mark}(m,p) \dots \text{search}(p):ms \Rightarrow m \text{ in } ms$

attribute blame to Trash

# slightly surprising behavior #5

label:social

Remove label

Inbox Promotions Social buy this! - My new 10:33 am

label:promotions

Remove label

Inbox Promotions Social buy this! - My new 10:33 am

label:social label:promotions

No messages matched your search. Try using [search options](#) such as sender, date, size and more.

violates Label's spec

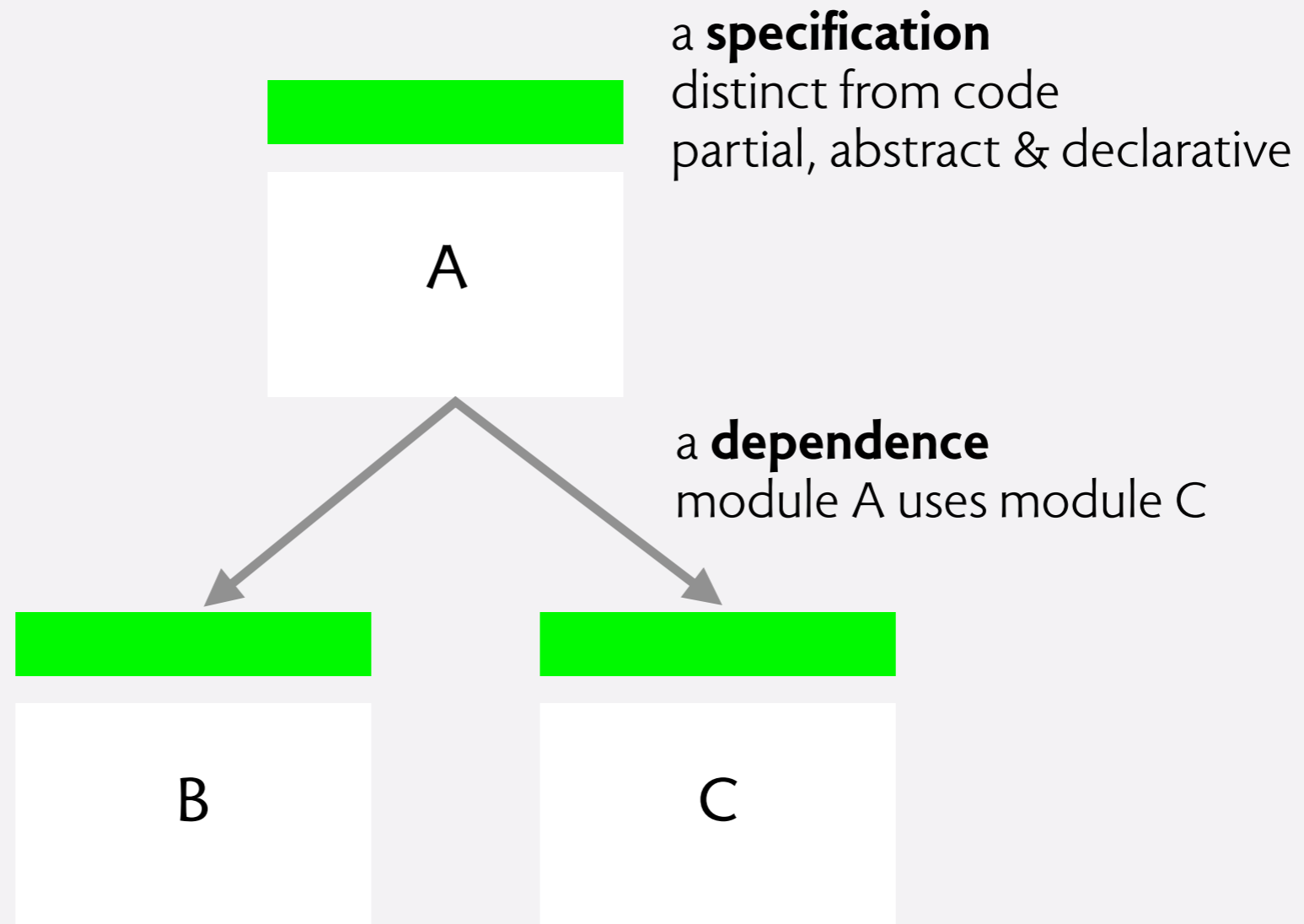
attribute blame to Category

# table of interactions

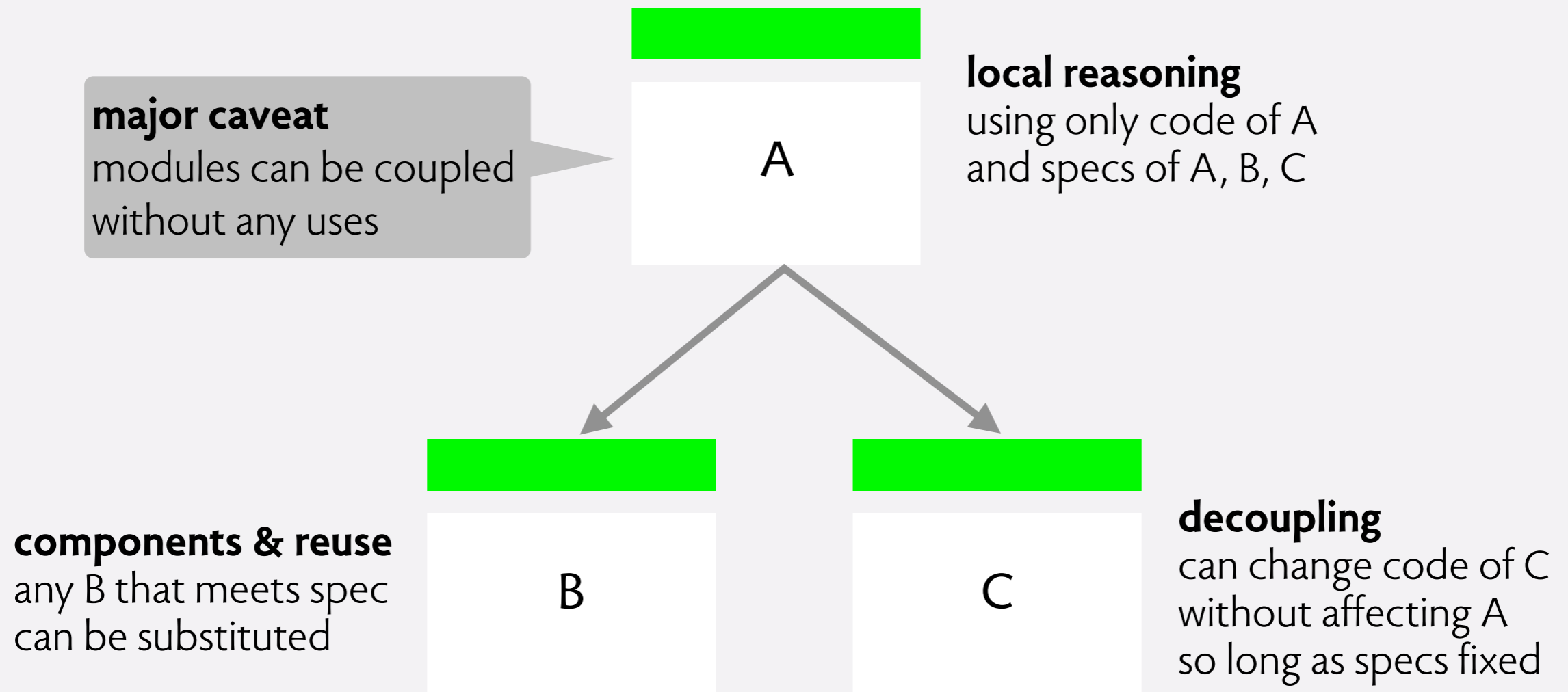
	Label	Category	Conversation	Trash
Label	-	breaks spec	breaks OP	breaks OP
Category	breaks spec	-	breaks spec	
Conversation			-	breaks OP
Trash				-

addendum:  
on specs

# what is a specification?



# what specifications gave us





# some specs matter more



## **top level specification**

determines the impact  
of the software in the world

# separating concerns

