a new way to think about specifications

Daniel Jackson · CSAIL, MIT

ABZ · June 7, 2018
a different project

Portraits of Resilience
Daniel Jackson
foreword by David A. Karp

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

**need**
the motivation for building the system

**specification**
the planned behavior of the system

**implementation**
the mechanisms of the system
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

correctness

implementation
the mechanisms of the system
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

implementation
the mechanisms of the system

pleasantness

correctness
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

implementation
the mechanisms of the system

pleasantness

correctness

what we devoted ourselves to
separating concerns

- need
  - the motivation for building the system
- specification
  - the planned behavior of the system
- implementation
  - the mechanisms of the system

what mattered more?
what we devoted ourselves to

pleasantness

correctness
<table>
<thead>
<tr>
<th>Primary</th>
<th>Social</th>
<th>Promotions</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (12) hacking meetups javascript - Hello again Be</td>
<td>11:48 am</td>
<td></td>
</tr>
</tbody>
</table>

**correct ⇒ useful?**
correct ⇒ useful?
correct ⇒ useful?

<table>
<thead>
<tr>
<th>Primary</th>
<th>Social</th>
<th>Promotions</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (12)</td>
<td>hacking</td>
<td>javascript - Hello again Ben</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>label: hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (12)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>label: meetups</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (12)</td>
</tr>
</tbody>
</table>
correct ⇒ useful?
correct ⇒ useful ?
Correct $\Rightarrow$ Useful?

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

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>me, Alyssa (13)</td>
<td>hacking, meetups, todo, javascript - Hello a</td>
</tr>
<tr>
<td></td>
<td>Andy from Google</td>
<td>Updates, Ben, welcome to your new Goog!</td>
</tr>
</tbody>
</table>

11:48 am  9:01 am
correct ⇒ useful?
correct ⇒ useful?
correct $\Rightarrow$ useful?
correct \Rightarrow useful?

- Empty Trash now (messages that have been in Trash more than 30 days will be automatically deleted)
- me, Alyssa (13)
- Andy from Google
- Updates
- Ben, welcome to your new Google

- label:todo
- There are no conversations with this label.

- label:todo label:trash
- me, Alyssa

- label:todo OR label:meetup

- Some messages in Trash or Spam match your search. View messages.
correct ⇒ useful?
correct ⇒ safe?
correct $\Rightarrow$ safe ?

airborne $\Leftrightarrow$ disabled

requirement

Airbus A320, Warsaw 1993
correct $\Rightarrow$ safe?

- WheelPulse $\Leftrightarrow$ disabled
- airborne $\Leftrightarrow$ disabled

specification

requirement

Airbus A320, Warsaw 1993
Airbus A320, Warsaw 1993

correct ⇒ safe?

airborne ⇔ ¬WheelPulse

¬WheelPulse ⇔ disabled

airborne ⇔ disabled

environment ∧ specification ⇒ requirement
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…
From: "TIG" <help@MIT.EDU>
Date: October 13, 2008 11:04:08 AM EDT
To: "Daniel Jackson" <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
From: "TIG" <help@MIT.EDU>
Date: October 13, 2008 11:04:08 AM EDT
To: "Daniel Jackson" <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
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
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
core concepts: a universal design strategy

architecture

graphic design

music

massing
core concepts: a universal design strategy

architecture

graphic design

identity

massing

music
core concepts: a universal design strategy

architecture

graphic design

identity

massing

mit media lab

music

motif
core concepts for software

- **Apple iPod**: core concepts: song, playlist
- **WhatsApp**: core concepts: post, group, call
- **Slack**: core concepts: message, channel, mention
- **Instagram**: core concepts: photo, follow, like
- **Adobe Photoshop**: core concepts: pixel map, layer/mask
- **Microsoft Word**: core concepts: paragraph, styles
- **InDesign**: core concepts: paragraph, styles, linkedBox, page
concept basics
what is a concept?
what is a concept?
what is a concept?

inventive
what is a concept?

- inventive
- purposeful
what is a concept?

- inventive
- purposeful
- behavioral
what is a concept?

- inventive
- purposeful
- behavioral
- self-contained
what is a concept?

- inventive
- purposeful
- behavioral
- self-contained
- reusable
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
inventive
purposeful
behavioral
self-contained
reusable
trash

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

purposeful
purpose is:
to undo deletions!

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

self-contained
synergistic with file system
but concept requires only set of objects

reusable
messages (Gmail)
photos (iPhoto)
posts (WordPress)
notes (Evernote)
<table>
<thead>
<tr>
<th></th>
<th>trash</th>
<th>reservation</th>
</tr>
</thead>
</table>
| 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

spec

operational principle
the trash concept

- purpose: allow undo of deletion
- spec
- operational principle
allow undo of deletion

**purpose**

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

**actions**
- new (): $X \triangleq \text{result} \in \text{all and all'} = \text{all} + \text{result}$
- del (x: X) $\triangleq \text{deleted'} = \text{deleted} + x$
- empty () $\triangleq \text{no deleted'} \text{ and all'} = \text{all} - \text{deleted}$

**spec**

showAll () : set $X \triangleq \text{result} = \text{all}$

**operational principle**
**the trash concept**

**purpose**
allow undo of deletion

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

**actions**
new (): $X \triangleq \text{result} \not \in \text{all}$ and all’ = all + result
del (x: X) \triangleq \text{deleted’} = \text{deleted} + x
empty () \triangleq \text{no deleted’ and all’} = \text{all} - \text{deleted}

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

**operational principle**
del(x) ... **not** empty() ... showAll():xs ⇒ x **in** xs
del(x) ... empty() ... showAll():xs ⇒ x **not in** xs
the label concept

purpose

spec

operational principle
the label concept

purpose: organize items for easy retrieval

spec

operational principle
the label concept

organize items for easy retrieval

**purpose**

**state** labels: \( X \rightarrow \text{Label} \)

**actions**
- mark \((x: X, p: \text{Label}) \triangleq \text{labels'} = \text{labels} + x \rightarrow p\)
- unmark \((x: X, p: \text{Label}) \triangleq \text{labels'} = \text{labels} - x \rightarrow p\)

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

**operational principle**
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 - $x \rightarrow p$

**spec**

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

**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

P1

P2

concepts

C1

C2
four ways to fail

unfulfilled purpose

overloaded concept

unmotivated concept

redundant concepts
my camera fuji x100s
image quality setting
image quality setting

- FINE
- NORMAL
- FINE+RAW
- NORMAL+RAW
- RAW
aspect ratio
aspect ratio
image size setting
<table>
<thead>
<tr>
<th>Image Size</th>
<th>Frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:2</td>
<td>664</td>
</tr>
<tr>
<td>16:9</td>
<td>681</td>
</tr>
<tr>
<td>1:1</td>
<td>702</td>
</tr>
<tr>
<td>3:2</td>
<td>707</td>
</tr>
<tr>
<td>16:9</td>
<td>719</td>
</tr>
<tr>
<td>1:1</td>
<td>734</td>
</tr>
<tr>
<td>3:2</td>
<td>746</td>
</tr>
</tbody>
</table>

Image size setting:

- **3:2**: 664 frames
- **16:9**: 681 frames
- **1:1**: 702 frames
- **3:2**: 707 frames
- **16:9**: 719 frames
- **1:1**: 734 frames
- **3:2**: 746 frames
image size setting

- 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

3264x3264 (11M)  702 FRAMES
image size setting

Shooting menu:
- Self-Timer: Off
- ISO: AUTO
- Image Size: L 1:1
- Image Quality: F+ RAW
- Dynamic Range: DR 100
- Film Simulation
- Film Simulation BKT
non-standard ratio + raw?
what you can’t do

non-standard aspect ratio + raw
even though raw images get nice nondestructive crop!
what you can’t do

non-standard aspect ratio + raw
even though raw images get nice nondestructive crop!
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]
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
piggybacking fuji camera

new purpose hacked onto old concept

image size
aspect ratio piggybacked on JPEG dimensions
piggybacking epson driver
piggybacking epson driver
piggybacking epson driver
piggybacking 

epson driver
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
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
emergent purpose

users find second purpose for concept

initial purpose: summarize content

to: Daniel Jackson <dnj@mit.edu>
re: Catch me if you can in real life!

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

to: csail-related@lists.csail.mit.edu
re: [csail-related] turn off the lights?

thanks to Shriram Krishnamurthi
users find second purpose for concept

initial purpose: summarize content

To: Daniel Jackson <dnj@mit.edu>
Re: Catch me if you can in real life!

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

thanks to Shriram Krishnamurthi

To: csail-related@lists.csail.mit.edu
Re: [csail-related] turn off the lights?

emergent purpose: group by conversation

your trip reservation

can’t label reservations from Expedia by trip

thanks to Eunsuk Kang
designer believes second purpose unnecessary
the
uniformity
rule
what makes a usable concept?

operational principle is uniform
always the same actions, irrespective of context
what makes a usable concept?

operational principle is uniform
always the same actions, irrespective of context
what makes a usable concept?

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

**unless** objs contains a text body object

quantified over state & args
non-uniformity

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>item</strong></td>
<td><strong>cost</strong></td>
</tr>
<tr>
<td>apples</td>
<td>$4</td>
</tr>
<tr>
<td>bananas</td>
<td>$2</td>
</tr>
<tr>
<td>grapes</td>
<td>$6</td>
</tr>
<tr>
<td>kiwis</td>
<td>$3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>item</strong></td>
<td><strong>cost</strong></td>
</tr>
<tr>
<td>apples</td>
<td>$4</td>
</tr>
<tr>
<td>bananas</td>
<td>$2</td>
</tr>
<tr>
<td><strong>cherries</strong></td>
<td></td>
</tr>
<tr>
<td>grapes</td>
<td>$6</td>
</tr>
<tr>
<td>kiwis</td>
<td>$3</td>
</tr>
</tbody>
</table>

$15
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)
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....
```
non-uniformity conversation

action applied to every message in conversation
non-uniformity conversation

action applied to every message in conversation unless message in other folder or action is reply...
kinds of non-uniformity

Keynote grouping unless objs contains a text body object

Fuji aspect ratio setting unless set to raw only mode

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

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

Twitter mention unless mention includes first character of tweet
kinds of non-uniformity

- Keynote grouping: unless `objs` contains a text body object
- Fuji aspect ratio setting: unless set to raw only mode
- Dropbox share folder: unless folder is ancestor or descendant of shared folder
- Git branch: unless working directory contains uncommitted file or...
- Twitter mention: unless mention includes first character of tweet
kinds of non-uniformity

- **Keynote grouping** unless `objs` contains a text body object
- **Fuji aspect ratio setting** unless set to raw only mode
- Dropbox share folder unless folder is ancestor or descendant of shared folder
- Git branch unless working directory contains uncommitted file or...
- Twitter mention unless mention includes first character of tweet
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...

- Twitter mention: unless mention includes first character of tweet
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
interpreting composite behavior

each action in composite system interpreted as zero or more actions in each concept
action is $\text{Label.show}(p) : ms$
where $p$ is the label $\text{sent}$
and $ms$ is the set of two messages listed
action is $\text{Label.show}(p): ms$
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 $\text{Label.mark}(m, p)$
where $p$ is the label sent
a simple criterion
projected behavior must satisfy concept spec:
∀ c: concept | ∀ t: traces(sys) | R_c(t) ∈ traces(c)
judging composite behavior

a simple criterion
projected behavior must satisfy concept spec:
∀ c: concept | ∀ t: traces(sys) | R_c(t) ∈ traces(c)
judging composite behavior

A simple criterion
projected behavior must satisfy concept spec:
∀ c: concept | ∀ t: traces(sys) | R_c(t) ∈ traces(c)
judging composite behavior

A simple criterion: projected behavior must satisfy concept spec:
\[ \forall c: \text{concept} \mid \forall t: \text{traces(sys)} \mid R_c(t) \in \text{traces}(c) \]
a simple criterion
projected behavior must satisfy concept spec:
\[ \forall c: \text{concept} \mid \forall t: \text{traces(sys)} \mid R_c(t) \in \text{traces}(c) \]
judging composite behavior

a simple criterion
projected behavior must satisfy concept spec:
\[ \forall c: \text{concept} \mid \forall t: \text{traces(sys)} \mid R_c(t) \in \text{traces}(c) \]
judging composite behavior

A simple criterion
projected behavior must satisfy concept spec:
\[ \forall c: \text{concept} \mid \forall t: \text{traces(sys)} \mid R_c(t) \in \text{traces}(c) \]
a simple criterion
projected behavior must satisfy concept spec:
∀ c: concept | ∀ t: traces(sys) | R_c(t) ∈ traces(c)
a simple criterion
projected behavior must satisfy concept spec:
\[ \forall c: \text{concept} \mid \forall t: \text{traces(sys)} \mid R_c(t) \in \text{traces}(c) \]
example gmail

violates spec of Label.search
action is \texttt{Label.search}(p):ms where \texttt{p} is the label sent and \texttt{ms} is the set of two messages listed

 violates spec of \texttt{Label.search}
action is \texttt{Label.search}(p)\texttt{: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 \texttt{Label.mark}(m, p) where \(p\) is the label sent

\textcolor{cyan}{violates spec of \texttt{Label.search}}
integrity violations

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
Deja Vu (Santiago Perez De Rosso)
library of polymorphic concepts, each implementing full stack
composed in HTML by linking actions

integrating concepts to make apps

\[
\begin{array}{cccccccccccccccc}
\text{app} & \text{Accord} & \text{ChoreStar} & \text{MapMIT} & \text{Rendezvous} & \text{SweetSpots} & \text{Potluck} & \text{GroceryShip} & \text{Lingua} & \text{LiveScorecard} \\
\hline
\text{Authentication} & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 \\
\text{Authorization} & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\text{Passkey} & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
\text{Market} & 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
\text{Rating} & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
\text{Follow} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Geolocation} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Post} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Comment} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Event} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Label} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Group} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Task} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Checklist} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Property} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Scoring} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\text{Chat} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\end{array}
\]
closing thoughts
finding bugs in design: what kind?

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

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

what designers actually use models for
simulating experience of finished product
to find unanticipated misfits
models in design vs engineering

what engineers use models for?
calculating properties, checking against higher level specs
to find bugs

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

shallow flaws
models in design vs engineering

what engineers use models for?
calculating properties, checking against higher level specs
to find bugs

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

Gmail

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: 14 hours ago
Details

javascript - Reminds you of the old days, eh?

9:14 pm
organizing messages
organizing messages
organizing messages

Google

label:hacking

Gmail

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
automating filtering
automating filtering
slightly surprising behavior #1
slightly surprising behavior #1
slightly surprising behavior #1
slightly surprising behavior #1
slightly surprising behavior #2

<table>
<thead>
<tr>
<th></th>
<th>Primary</th>
<th>Social</th>
<th>Promotions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>me, Alyssa (12)</td>
<td>hacking</td>
<td>javascript</td>
</tr>
<tr>
<td></td>
<td></td>
<td>meetups</td>
<td>Hello again B</td>
</tr>
</tbody>
</table>

11:48 am
slightly surprising behavior #2
slightly surprising behavior #2
slightly surprising behavior #2

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Label</th>
<th>Subject</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa</td>
<td>hacking</td>
<td>javascript - Hello again Ben</td>
<td>11:48 am</td>
</tr>
<tr>
<td>me, Alyssa</td>
<td>meetups</td>
<td>javascript - Hello again Ben</td>
<td>9:43 am</td>
</tr>
<tr>
<td>me, Alyssa</td>
<td>hacking</td>
<td>javascript - Hello again Ben</td>
<td>9:58 am</td>
</tr>
</tbody>
</table>

No messages matched your search. Try using search options such as sender, date, size and more.
slightly surprising behavior #3
slightly surprising behavior #3
slightly surprising behavior #4
slightly surprising behavior #4

<table>
<thead>
<tr>
<th>Message</th>
<th>Status</th>
<th>Subject</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (13)</td>
<td></td>
<td>hacking, meetups, todo, javascript - Hello a</td>
<td>11:48 am</td>
</tr>
<tr>
<td>Andy from Google</td>
<td>Updates</td>
<td>Ben, welcome to your new Google!</td>
<td>9:01 am</td>
</tr>
</tbody>
</table>
slightly surprising behavior #4

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

- Andy from Google  Updates  Ben, welcome to your new Google!
  9:01 am

label:todo

There are no conversations with this label.
**slightly surprising behavior #4**

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

<table>
<thead>
<tr>
<th>Message</th>
<th>Labels</th>
<th>Sender</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (13)</td>
<td>hacking, meetups, todo, javascript</td>
<td>Andy from Google</td>
<td>11:48 am</td>
</tr>
<tr>
<td>Andy from Google</td>
<td>Updates</td>
<td>Ben, welcome to your new Google</td>
<td>9:01 am</td>
</tr>
</tbody>
</table>

There are no conversations with this label.

<table>
<thead>
<tr>
<th>Message</th>
<th>Labels</th>
<th>Sender</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa</td>
<td>Trash, hacking, meetups, todo, javascript</td>
<td>10:11 am</td>
<td></td>
</tr>
</tbody>
</table>
slightly surprising behavior #4

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  
  11:48 am

- 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

- 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

<table>
<thead>
<tr>
<th>Star</th>
<th>Name</th>
<th>Promotions</th>
<th>Message</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Alyssa P. Hacker</td>
<td>Promotions</td>
<td>buy this! - My new JS book is out</td>
<td>10:33 am</td>
</tr>
</tbody>
</table>
slightly surprising behavior #5

Alyssa P. Hacker: buy this! - My new JS book is out
10:33 am

Social: buy this! - My new JS book is out!
10:33 am
slightly surprising behavior #5
slightly surprising behavior #5
slightly surprising behavior #5
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

Google

Gmail

Inbox
Starred
Sent Mail
Drafts
Trash
Categories

COMPOSE

in:sent

javascript

Inbox hacking

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

Ben Bitdiddle <benito.bitdiddle@gmail.com>
to Alyssa
Yes, it does.
9:40 PM (7 minutes ago)
slightly surprising behavior #1

violates Label’s operational principle:
not mark(m,p) ... search(p):ms ⇒ m not in ms
slightly surprising behavior #1

violates Label’s operational principle: not mark(m,p) ... search(p):ms ⇒ m not in ms

attribute blame to Conversation
slightly surprising behavior #2
slightly surprising behavior #2

violates nothing: expected behavior of Label and Conversation
slightly surprising behavior #4

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

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (13)</td>
<td>hacking</td>
<td>todo</td>
<td></td>
</tr>
<tr>
<td>Andy from Google</td>
<td>Updates</td>
<td>Ben, welcome to your new Google</td>
<td></td>
</tr>
</tbody>
</table>

There are no conversations with this label.
slightly surprising behavior #4

violates Label’s operational principle: mark(m,p) ... search(p):ms ⇒ m in ms
slightly surprising behavior #4

<table>
<thead>
<tr>
<th>Label</th>
<th>Conversation Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>me, Alyssa (13)</td>
<td>hacking meetups todo javascript - Hello</td>
</tr>
<tr>
<td>Andy from Google</td>
<td>Updates Ben, welcome to your new Google</td>
</tr>
</tbody>
</table>

violates Label’s operational principle: 
\[ \text{mark}(m,p) \ldots \text{search}(p):ms \Rightarrow m \in ms \]

attribute blame to Trash
slightly surprising behavior #5

No messages matched your search. Try using search options such as sender, date, size and more.
slightly surprising behavior #5

<table>
<thead>
<tr>
<th>label: social</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alyssa P. Hacker</td>
<td>Inbox</td>
<td>Promotions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>label: promotions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alyssa P. Hacker</td>
<td>Inbox</td>
<td>Promotions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>label: social label: promotions</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

No messages matched your search. Try using search options such as sender, date, size and more.

violates Label’s spec
slightly surprising behavior #5

violates Label’s spec

attribute blame to Category
<table>
<thead>
<tr>
<th></th>
<th>Label</th>
<th>Category</th>
<th>Conversation</th>
<th>Trash</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>-</td>
<td>breaks spec</td>
<td>breaks OP</td>
<td>breaks OP</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>breaks spec</td>
<td>-</td>
<td>breaks spec</td>
<td></td>
</tr>
<tr>
<td><strong>Conversation</strong></td>
<td></td>
<td>-</td>
<td>-</td>
<td>breaks OP</td>
</tr>
<tr>
<td><strong>Trash</strong></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
</tr>
</tbody>
</table>
addendum: on specs
what is a specification?

A specification is distinct from code. It is partial, abstract, and declarative. For example, module A depends on module C, as module A uses module C.
what specifications gave us

- **local reasoning**: using only code of A and specs of A, B, C
- **decoupling**: can change code of C without affecting A so long as specs fixed
- **components & reuse**: any B that meets spec can be substituted
- **major caveat**: modules can be coupled without any uses
some specs matter more

**top level specification**
determines the impact of the software in the world
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

implementation
the mechanisms of the system
separating concerns

**need**
the motivation for building the system

**specification**
the planned behavior of the system

**correctness**

**implementation**
the mechanisms of the system
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

correctness

implementation
the mechanisms of the system

pleasantness
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

implementation
the mechanisms of the system

pleasantness

what we devoted ourselves to

correctness
separating concerns

need
the motivation for building the system

specification
the planned behavior of the system

implementation
the mechanisms of the system

pleasantness

what we devoted ourselves to

what mattered more?

correctness