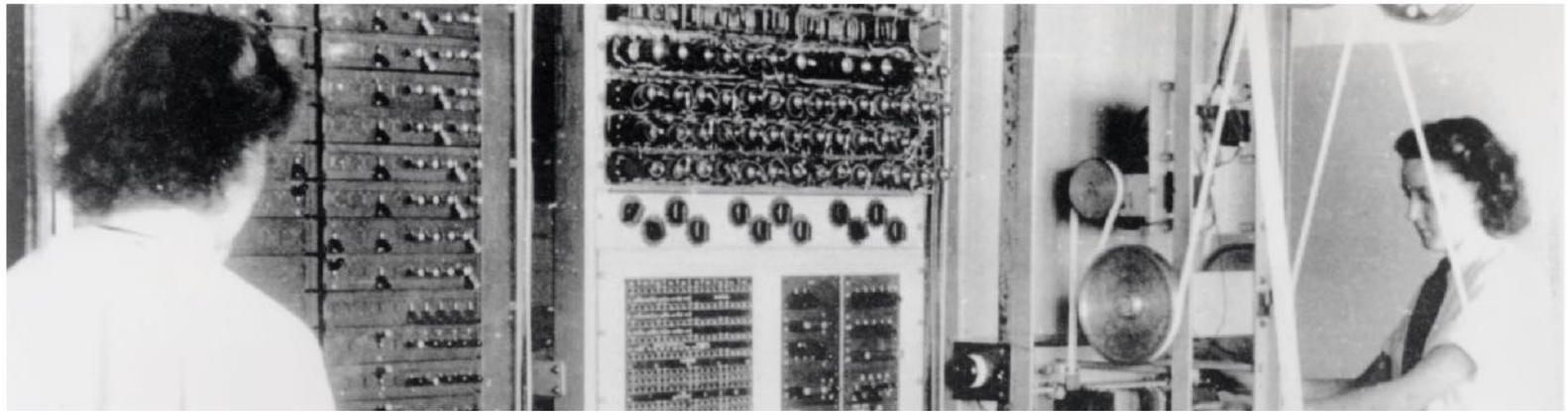
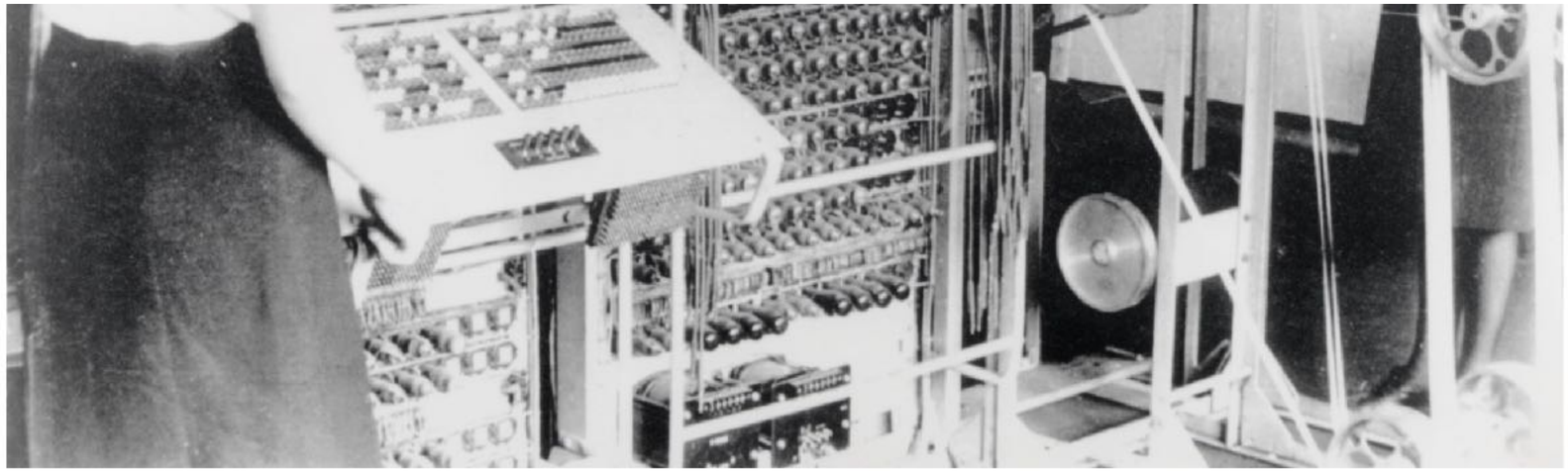
Harvard John A. Paulson
School of Engineering
and Applied Sciences

PL/HCI Seminar (252R/279R)

MW 12-1:15 PM in LISE 303



Making communicating with computers more accessible: easier, faster, and safer



Welcome!

- This is a graduate course; undergrads are welcome.
  - can have taken 152 *or* 179 and be just fine, not necessarily both
- You (as a student presenter) will present and lead discussion for at least one paper
- You (as a non-presenting student) will post questions and a summary of the design arguments by Friday of the previous week
- Key learning outcomes:
  - (279r) to look at scientific publications, identify the core design arguments, write new design arguments, and evaluate them
  - (252r) understand, design and implement language abstractions for solving a task
- Group projects will be composed of both “HCI folks” and “PL folks”

Harvard John A. Paulson
School of Engineering
and Applied Sciences

PL/HCI Seminar (252R/279R)

Why PL–HCI Matters

A case study in **types**

Medical infrastructure – Elena
Software engineering – Nada

Harvard John A. Paulson
School of Engineering
and Applied Sciences

PL/HCI Seminar (252R/279R)

Medical infrastructure

Hospitals


診症區域 只可一人陪同
CONSULTATION AREA
ONE ACCOMPANIAN ONLY
分流站
Triage Station
Approximate Waiting Time for consultation :
Triage Category
Waiting Time
Urgent
0.5
hour
Semi-Urgent
3
hours
Non-Urgent
4
hours

Suburban General Hospital

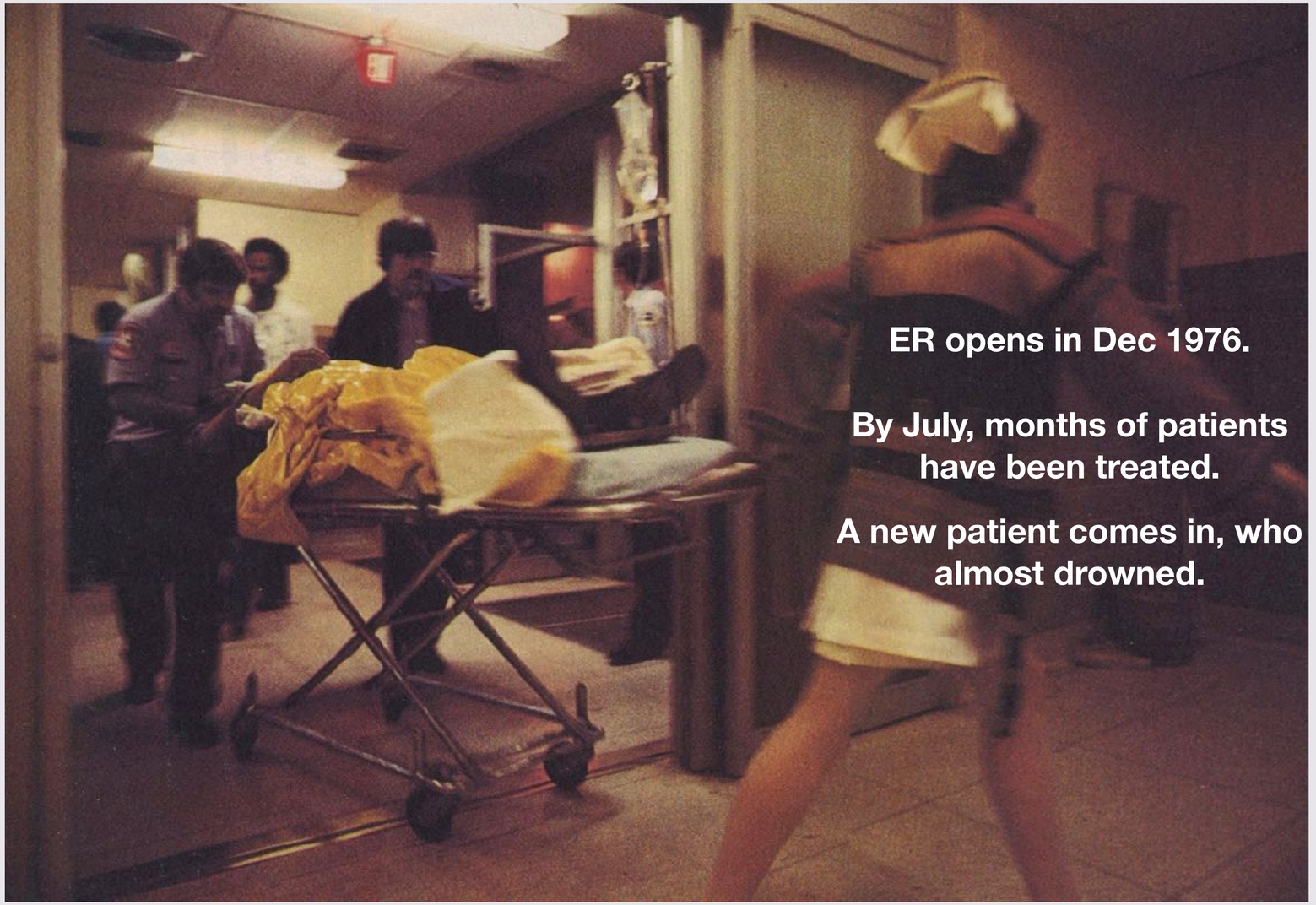
141-bed osteopathic hospital in Philadelphia

Suburban General Hospital

141-bed osteopathic hospital in Philadelphia

Suburban General Hospital

141-bed osteopathic hospital in Philadelphia



Suburban General Hospital

141-bed osteopathic hospital in Philadelphia

ER opens in Dec 1976.

By July, months of patients have been treated.

A new patient comes in, who almost drowned.

Suburban General Hospital

141-bed osteopathic hospital in Philadelphia

ER opens in Dec 1976.

By July, months of patients have been treated.

A new patient comes in, who almost drowned.

Philadelphia Inquirer
Sunday April 23, 1978

Thirteen deaths—Here is a list of suits in mix-up

In September 1977, a three-man panel appointed by Acting Montgomery County Coroner Charles Thomes studied the hospital records of 98 patients who were pronounced dead at Suburban General Hospital during the seven months when the oxygen and nitrous oxide gas lines into the emergency rooms were inadvertently crossed.

Of those 98 patients, the panel concluded that the deaths of six patients "were causally related to the administration of nitrous oxide," and that in three of those cases it was the immediate cause of death. The panel found another six cases "in which there are insufficient data to evaluate the effects, if any, of nitrous oxide." (In the other cases, the study found that the patients had not been treated in the emergency room or had not required the use of oxygen.)

The 12 cases account for all but one of the lawsuits filed so far with the state's Office of Medical Malpractice Arbitration.

The 13th suit was filed by relatives of a patient who, the panel concluded, had "died from causes not related to the administration of nitrous oxide."

Following are brief accounts of each case, taken from information outlined in the suits, interviews with attorneys and news accounts.

These are the three patients whose immediate cause of death was found by the coroner's panel to be the administration of nitrous oxide instead of oxygen:

GLENN BOONE, 10, of Whitpain Township, who was rushed to the emergency room on Dec. 19, 1976, after suffering burns over 90 percent of his body in a gasoline explosion in his parents' garage. He was having trouble breathing so doctors cut a hole in his throat and put a tube in to deliver oxygen. He died seven hours later.

CHARLES SPANGLER, 71, a retired insurance agent, who awoke at 2 a.m. on Feb. 12, 1977, with a severe coughing spell. An ambulance took him to the emergency room. He died an hour later. Initially, his death certificate showed that Spangler died of heart failure, but the Thomas panel amended it to show that by receiving nitrous oxide instead of oxygen, Spangler died of a lack of oxygen.

In papers filed with the malpractice board, Spangler's wife said he had been in good health, although he had high blood pressure.

ISADORE L. DUBIN, 54, of Arboretum Road, Wyncote, a dentist, complained on the morning of May 30, 1977, that he was not feeling well. The State Police took him to the emergency room at 8:36 a.m. and called his wife at home. By the time she arrived, he was dead. He had been given nitrous oxide by nose tube and face mask from the oxygen outlet and died at 9:25 a.m., according to the suit.

Suits were filed by relatives of the three following patients whose deaths, according to the Thomes panel, "were causally related to the administration of nitrous oxide" and "whose underlying condition was seriously aggravated by nitrous oxide":

PAUL HORWITZ, 47, of the 2700 block of Aspen Circle, Norristown, was a microbiologist at Wyeth Laboratories, according to the suit filed by his wife and two sons. He was taken to the emergency room suffering apparent heart trouble at 2:10 a.m., March 5, 1977, and given nitrous oxide from the oxygen outlet. He died at 3:28 a.m.

JOSEPHINE CIANCIULLI, 43 of the 300 block of Grove St., Bridgeport, had a fainting spell at home at 2 p.m. April 15, 1977. An ambulance took her to the emergency room. She was given nitrous oxide, which caused oxygen deprivation "which seriously aggravated her existing clinical state . . . and accelerated her death at approximately 3:35 p.m.," the suit says.

PHILOMENA HEWITT, 51, a laundry supervisor at Norristown State Hospital, was watching television in her home in the 500 block of Kohn St., Norristown, when she began a severe coughing spell. Because her doctor was not available, she was taken to Suburban General's emergency room. Her husband waited outside the cubicle where she was being treated. An hour after she arrived, a doctor emerged and said she was dead. The suit claims she had no previous medical condition that endangered her life.

Six other persons were inadvertently treated with nitrous oxide instead of oxygen, but the coroner's panel concluded that there was "insufficient data to evaluate the effects, if any," of the lack of oxygen. The survivors of all six of the following patients have sued:

GRACE HICKS, 61, of Norristown, was taken to the emergency room on the morning of Jan. 17, 1977, suffering from a degenerative muscular disease, amyotrophic sclerosis, known as "Lou Gehrig's disease." Because she was having a choking attack, her son immediately asked that she receive oxygen. She died minutes after she was administered nitrous oxide instead of oxygen, the suit claims.

WILLIAM F. DETTERLINE JR., 71, a retired laborer, was taken to the emergency room on Feb. 22, 1977, suffering an apparent heart attack. He was short of breath. He died at 8:15 p.m., less than an hour after he arrived, after treatment with introus oxide from the oxygen outlet.

MARTIN J. SMITH, 43, of Glen Oak Road, Jeffersonville, was taken to the emergency room on March 6, 1977, and died of a heart attack at 10:19 a.m., after receiving nitrous oxide instead of oxygen, the suit alleges.

MARIA GIORI, 65, of Launfall Road, Plymouth Meeting, was taken to the emergency room after dawn on March 18, 1977. She was lucid when she arrived, and was hooked up by mask to the oxygen line at 6:05 a.m. She died 24 minutes later.

GEORGE PURSLEY, 66, of Oaklyn Ave., Norristown, a retired housepainter with a history of high blood pressure, complained of dizziness and weakness and was taken to the emergency room on March 5, 1977, at 2:35 a.m. At 3:30 a.m., he was given nitrous oxide insead of oxygen and his heart stopped seven minutes later, according to the suit. He was pronounced dead at 3:45 a.m.

CHARLES J. VENEZIA SR., 62, was taken to the emergency room on April 6, 1977, after his emphysema flared up. He was given nitrous oxide from the oxygen outlet and was admitted to the hospital after suffering a heart attack in the emergency room, according to the family's account. He was unconscious for 12 days and died April 18.

The 13th suit was filed by the widow of Charles Darden, 75, who was treated with nitrous oxide in the emergency room after complaining of chest pains. He died in the hospital two days later Darden was listed in the panel's report as one of the patients whose death was not related to the administration of nitrous oxide.

The survivors of three other patients who died in the hospital have filed "notice complaints" with the medical malpractice board. In this way, plaintiffs who are uncertain whether they have grounds to sue may reserve the right to do so after the one-year statute of limitations following the patient's death runs out. Those patients were:

ANTHONY McNAW, 71, of Township Line, Gwynedd Valley, who died Feb. 21, 1977. The coroner's panel also included him among those whose deaths were from causes not related to the administration of nitrous oxide.

LOUISE S. COPLEY, 71, of Walnut Street, Norristown, who died March 22, 1977, after being treated in the emergency room five days earlier. It is not clear whether she received nitrous oxide. She was described in hospital records as suffering from advanced heart disease.

ROBERT J. McLOUGHLIN, 52, was a "respiratory cripple" who required oxygen therapy at home, according to his family's attorney, Herbert Kolsby. After complaining of pain, he was taken to the emergency room at 7:45 a.m. Dec. 21, 1976, and treated with nitrous oxide instead of oxygen. He died in the hospital two days later.

While recognizing that McLoughlin was a very sick man, Kolsby said of his case: "I can hardly take the position he would have been a gold medalist at the next Olympics, but on the issue (of being deprived of oxygen in the emergency room), I probably have the best case. If ever there was someone who hungered for oxygen, it was him."

—Linda S. Herskowitz

How the gas mix-up was discovered

The crossed oxygen and nitrous oxide gas lines in Suburban General Hospital's emergency room were discovered on July 6, 1977, by Dr. Leonard Becker, the hospital's chief anesthesiologist.

Becker had been called to the emergency room to treat a 2-year-old girl who had nearly drowned. He was baffled when the child inexplicably turned blue after being given what was supposed to be 100 percent oxygen from the central supply line. When he administered oxygen from a portable unit, the child's normal color returned.

Becker then inhaled deeply from the mask he had put on the child's face and realized that he was anesthetizing himself.

Hospital officials found the answer in the tangled gas lines concealed behind the wall of the new emergency room, which had opened on Dec. 15, 1976. The lines had been crossed in the construction. In the period before the mix-up was discovered, about 300 persons had been treated with what was thought to be oxygen.

On Aug. 1, the mix-up was disclosed publicly by William K. Myrtetus, the director of the state's Catastrophe Loss Fund, an insurance pool for medical facilities. Myrtetus had just been notified by hospital officials.

During the next several days, hospital and public officials gave wildly fluctuating estimates of how many deaths might be directly or in part related to the mix-up. Myrtetus speculated that as many as 35 deaths might have resulted.

Charles E. Thomes, Montgomery County's acting coroner, soon appointed a panel of medical specialists to study hospital records and to determine how many deaths were related to oxygen deprivation.

Their report, issued in September, concluded that a total of six deaths were related to the mix-up in the gas lines and that in six other cases information was too sketchy to determine whether the patients had died because they received the wrong gas.

The hospital's own hired consultant, Dr. Cyril H. Wecht, Allegheny County coroner, concluded that five deaths were related to the mix-up.

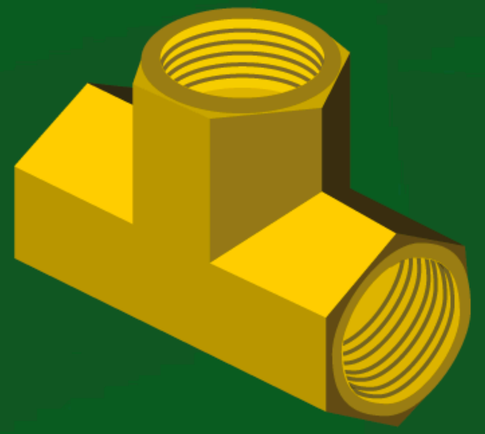
The hospital and one of its staff doctors sued Thomes in November, charging that his panel's report had subjected them to "public scandal and disgrace." No trial date on that has been set.

The gas mix-up 8 months later

HOSPITAL, From 1-K

fendants except Suburban General have named other people and firms as additional defendants, contending that they are at least in part responsible for the mix-up. ("It's typical lawyer work to name everyone in sight," said one plaintiff's attorney.)

most prominent malpractice attorney, is handling four of the cases against Suburban General and said emphatically that he expected that "it's all going to end up in Common Pleas Court, where the cases should have been in the first place. No one (of the defendants) is going to agree



Medical Gas Systems Installation

You Need to Know for Safety

CHT
WORLD CLASS HEALTHCARE COMPLIANCE

Piping System Controls	Band	Tape Colors	Stenciled Legends
Oxygen	Green	White w/ Green Letters	Oxygen or O2
Nitrous Oxide	Blue	Blue w/ White Letters	Nitrous Oxide or N2O
Medical Vacuum	White	Yellow w/ Black Letters	Medical Vacuum or VAC
Nitrogen	Black	Black w/ White Letters	Nitrogen or NIT
Carbon Dioxide	Gray	Gray w/ Black Letters	Carbon Dioxide or CO2
Medical Air	Yellow	White & Black w/ Contrast Letters	Medical Air or Med Air
Medical Anesthetic Gas Disposal	Violet	Violet w/ White Letters	WAGD

U.S. Department of Veterans Affairs

Mix-Ups

- **CO_2 and O_2:** A grayish green cylinder was confused for a greenish gray cylinder that resulted in a patient inhaling CO_2 during transport instead of oxygen. The use of universal adaptors (universal adaptors override the pin indexing system on the cylinder) contributed to this event.
- **CO_2/O_2 and CO_2:** Insufflation of the body cavity for arthroscopy is done with CO_2 as the gas will not sustain combustion and is easily absorbed by the body. A gray and green CO_2/O_2 cylinder was confused with the gray CO_2 cylinder that resulted in an internal body cavity fire when a surgical laser was used. The CO_2/O_2 gas will support combustion.

Oxygen Not Available

- It isn't always apparent whether an oxygen cylinder is full, partially full, or empty. In cases where the cylinder valve is closed and the regulator valve is open (see photograph; click on photo for larger view), no pressure will register on the pressure gauge. Staff in a hurry has assumed the cylinder is empty when in fact it is full.
- In some cases the O_2 cylinder is believed to be empty when trapped pressure in regulator is bled off by opening the flow meter/regulator valve when the cylinder valve is in the closed position.
- You can't always tell by just looking at the valve if it's open or closed. Valves controlling the oxygen flow are not indicating type valves. What's an indicating valve? See: A Brief History of Indicating Valves for Fire Protection *† for further information on this topic.

Cylinder goes ballistic

- Ferromagnetic O_2 cylinders introduced into the MRI environment can inadvertently be turned into missiles when they are drawn into the magnet. For more information on projectile hazards in and around MRIs see our MRI hazards page.
- A second way a cylinder can be turned into a missile is to fracture the cylinder. Escaping gas will propel the cylinder with enough force to penetrate cinder block walls.

Case Studies

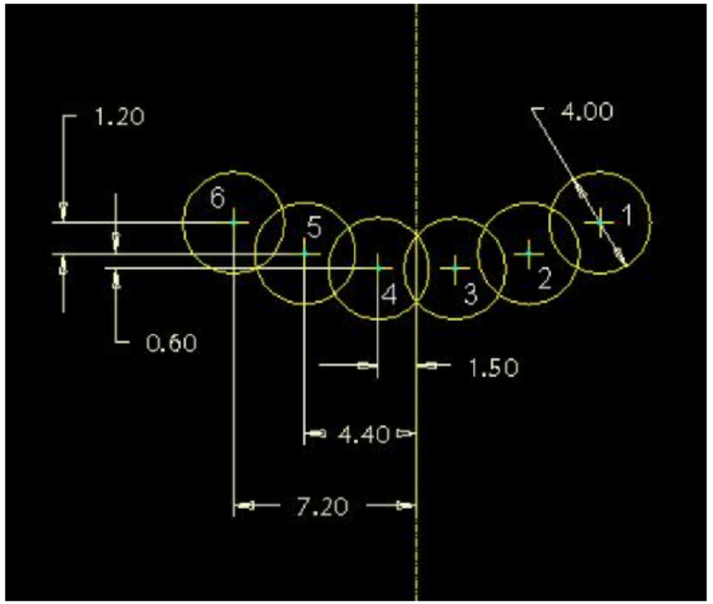
From FDA Manufacturer and User Facility Device Experience Database (MAUDE), ECRI, and VA databases

- An "E" cylinder containing CO_2 was mistaken for O_2 and was used during patient transport - he died. The modified O_2 regulator had been modified to fit "grayish" O_2 cylinder that really contained CO_2. This event emphasizes the point that cylinder color alone cannot be used to confirm the content of the cylinder.

Pin Index Safety System

From Wikipedia, the free encyclopedia

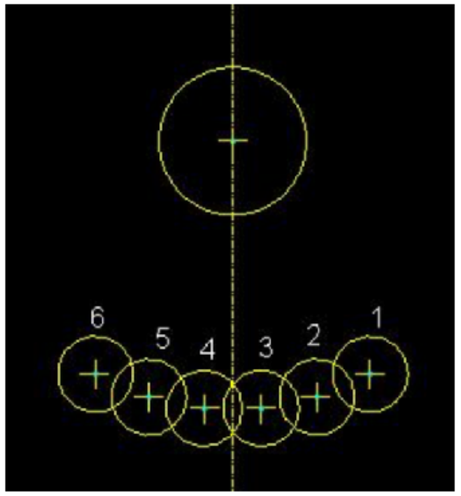
"PISS" redirects here. For other uses, see Piss (disambiguation).



The **Pin Index Safety System,** or PISS, is a means of connecting high pressure cylinders containing medical gases to a regulator or other utilization equipment. It uses geometric features on the valve and yoke to prevent mistaken use of the wrong gas. This system is widely used worldwide for anesthesia machines, portable oxygen administration sets, and inflation gases used in surgery.

Contents [hide]

1 Concept
2 Pin index configurations
3 International Standards
4 Limitations
5 Alternative systems
6 Blanking Plugs
7 See also
8 References



Concept [edit]

The pin index safety system uses a face seal between the cylinder valve and the associated yoke clamp. There are two holes in specific positions on the cylinder valve body below the outlet port , in positions associated with the gas mixture, which prevent connection of the cylinder to a yoke or pressure regulator with a mis-matched set of pins. The holes accept pins 4 mm diameter by 6 mm long which are correctly aligned with the holes.[1]

Pin index configurations [edit]

Each gas cylinder has a pin configuration to fit its respective gas yoke. Refer to the diagram for pin numbers; dimensions are in millimeters.

- O_2: 2,5[2][3][1]
- N_2O: 3,5[2][3][1]

U.S. Department of Veterans Affairs

Mix-Ups

- **CO_2 and O_2:** A grayish green cylinder was confused for a greenish gray cylinder that resulted in a patient inhaling CO_2 during transport instead of oxygen. The use of universal adaptors (universal adaptors override the pin indexing system on the cylinder) contributed to this event.
- **CO_2/O_2 and CO_2:** Insufflation of the body cavity for arthroscopy is done with CO_2 as the gas will not sustain combustion and is easily absorbed by the body. A gray and green CO_2/O_2 cylinder was confused with the gray CO_2 cylinder that resulted in an internal body cavity fire when a surgical laser was used. The CO_2/O_2 gas will support combustion.

Oxygen Not Available

- It isn't always apparent whether an oxygen cylinder is full, partially full, or empty. In cases where the cylinder valve is closed and the regulator valve is open (see photograph; click on photo for larger view), no pressure will register on the pressure gauge. Staff in a hurry has assumed the cylinder is empty when in fact it is full.
- In some cases the O_2 cylinder is believed to be empty when trapped pressure in regulator is bled off by opening the flow meter/regulator valve when the cylinder valve is in the closed position.
- You can't always tell by just looking at the valve if it's open or closed. Valves controlling the oxygen flow are not indicating type valves. What's an indicating valve? See: A Brief History of Indicating Valves for Fire Protection *† for further information on this topic.

Cylinder goes ballistic

- Ferromagnetic O_2 cylinders introduced into the MRI environment can inadvertently be turned into missiles when they are drawn into the magnet. For more information on projectile hazards in and around MRIs see our MRI hazards page.
- A second way a cylinder can be turned into a missile is to fracture the cylinder. Escaping gas will propel the cylinder with enough force to penetrate cinder block walls.

Case Studies

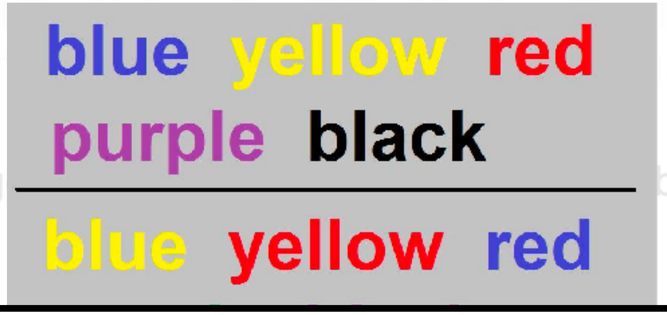
From FDA Manufacturer and User Facility Device Experience Database (MAUDE), ECRI, and VA databases

- An "E" cylinder containing CO_2 was mistaken for O_2 and was used during patient transport - he died. The modified O_2 regulator had been modified to fit "grayish" O_2 cylinder that really contained CO_2. This event emphasizes the point that cylinder color alone cannot be used to confirm the content of the cylinder.

U.S. Department of Veterans Affairs

Root Causes and Other Factors

- The most obvious cue for staff on the contents of a gas cylinder is the cylinder color, however, the color may be misleading or misunderstood. The cylinder label is the primary means of identifying the cylinder content. Follow directions and labels first - not color or other cues (e.g., storage location)… To be truly effective, CGA/ECRI recommends that the label be overwhelming in size.
- If there is a mismatch between the color of the cylinder and the cylinder content, for example a gray cylinder that contains oxygen or a green cylinder that contains nitrogen, this is a guarantee that future problems will occur. For more information on color mismatch confusion and how humans cannot ignored conflicting inputs see the "Stroop Effect" exercises*† a… de as many cues that a cylinder does not contain 100% O_2 as possible for … , store separately, transport in "odd-shaped" wheel cart).
- Text labels on cylinder can be damag… ble; if the label cannot be reliably read the cylinder should not be used.



Next Steps

- Color-coding may be misleading and is not ideal for use in identifying medical gases., NCPS will work with CGA and FDA to determine optimal labeling without use of color for coding on cylinders.

Philadelphia Inquirer
Sunday April 23, 1978

4-K Sunday, April 23, 1978 Philadelphia Inquirer

Thirteen deaths—Here is a list of suits in mix-up

In September 1977, a three-man panel appointed by Acting Montgomery County Coroner Charles Thomes studied the hospital records of 98 patients who were pronounced dead at Suburban General Hospital during the seven months when the oxygen and nitrous oxide gas lines into the emergency rooms were inadvertently crossed.

Of those 98 patients, the panel concluded that the deaths of six patients "were causally related to the administration of nitrous oxide," and that in three of those cases it was the immediate cause of death. The panel found another six

lance took him to the emergency room. He died an hour later. Initially, his death certificate showed that Spangler died of heart failure, but the Thomas panel amended it to show that by receiving nitrous oxide instead of oxygen, Spangler died of a lack of oxygen.

In papers filed with the malpractice board, Spangler's wife said he had been in good health, although he had high blood pressure.

ISADORE L. DUBIN, 54, of Ar
boretum Road, Wyncote, a dentist,
complained on the morning of May
30, 1977, that he was not feeling well.
The State Police took him to the

Hospital, was wat
her home in the
St., Norristown, w
severe coughing
doctor was not a
taken to Suburba
gency room. Her h
side the cubicle wh
treated. An hour
a doctor emerged
dead. The suit cl
previous medical
dangered her life.

Six other perso
tently treated wi
instead of oxyge
ner's panel conc

The Telegraph

HOME | NEWS | S

News

UK World Politics Science | Education | Health Brexit | Royals | Investigatio

U.S.

Medical Record Mix-Ups a Common Problem, Study Finds

The opportunities for the mistakes, which can be deadly, are increasing as health care becomes more complex

By Melinda Beck

Sept. 25, 2016 7:00 p.m. ET

A patient in cardiac arrest was mistakenly not resuscitated because clinicians confused him with a patient who had a do-not-resuscitate order on file.

Another patient was given an okay to undergo surgery based on a different patient's records and was found dead in his hospital room the next day.

Such patient-identification mix-ups are common...

mid 400 errors as NHS switch off oxygen

Save

8 months later

HOSPITAL, From 1-K

fendants except Suburban General have named other people and firms as additional defendants, contending that they are at least in part responsible for the mix-up. ("It's typical lawyer work to name everyone in sight," said one plaintiff's attorney.)

most prominent malpractice attorney, is handling four of the cases against Suburban General and said emphatically that he expected that "it's all going to end up in Common Pleas Court, where the cases should have been in the first place. No one (of the defendants) is going to agree

Philadelphia Inquirer
Sunday April 23, 1978

4-K Sunday, April 23, 1978 Philadelphia Inquirer

Thirteen deaths—Here is a list of suits in mix-up

In September 1977, a three-man panel appointed by Acting Montgomery County Coroner Charles Thomes studied the hospital records of 98 patients who were pronounced dead at Suburban General Hospital during the seven months when the oxygen and nitrous oxide gas lines into the emergency rooms were inadvertently crossed.

Of those 98 patients, the panel concluded that the deaths of six patients "were causally related to the administration of nitrous oxide," and that in three of those cases it was the immediate cause of death. The panel found another six

lance took him to the emergency room. He died an hour later. Initially, his death certificate showed that Spangler died of heart failure, but the Thomas panel amended it to show that by receiving nitrous oxide instead of oxygen, Spangler died of a lack of oxygen.

In papers filed with the malpractice board, Spangler's wife said he had been in good health, although he had high blood pressure.

ISADORE L. DUBIN, 54, of Arboretum Road, Wyncote, a dentist, complained on the morning of May 30, 1977, that he was not feeling well. The State Police took him to the

Hospital, was wat
her home in the
St., Norristown,
severe coughing
doctor was not
taken to Suburba
gency room. Her
side the cubicle wh
treated. An hour
a doctor emerged
dead. The suit cl
previous medical
dangered her life.

*Six other perso
tently treated wi
instead of oxyge
ner's panel conc*

The Telegraph

HOME | NEWS | S

News

UK World Politics Science | Education | Health Brexit | Royals | Investigatio

U.S.

Medical Record Mix-Ups a Common Problem, Study Finds

The opportunities for the mistakes, which can be deadly, are increasing as health care becomes more complex

By Melinda Beck

Sept. 25, 2016 7:00 p.m. ET

A patient in cardiac arrest was mistakenly not resuscitated because clinicians confused him with a patient who had a do-not-resuscitate order on file.

Another patient was given an okay to undergo surgery based on a different patient's records and was found dead in his hospital room the next day.

Such patient-identification mix-ups are common...

nid 400 errors as NHS switch off oxygen

Save

8 months later

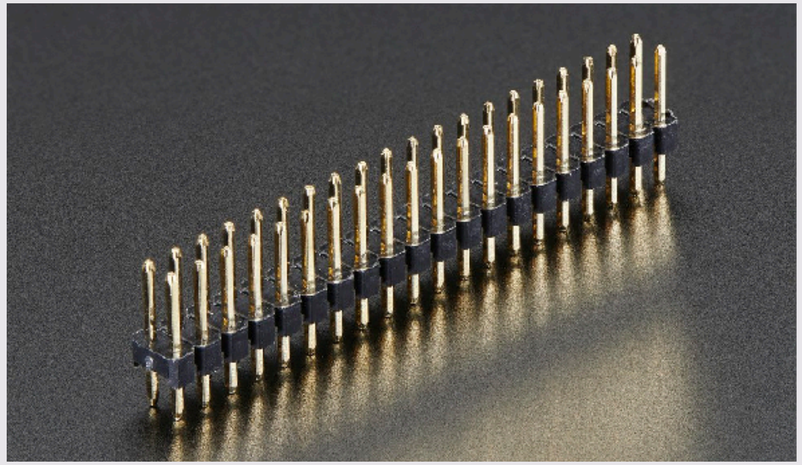
HOSPITAL, From 1-K

fendants except Suburban General have named other people and firms as additional defendants, contending that they are at least in part responsible for the mix-up. ("It's typical lawyer work to name everyone in sight," said one plaintiff's attorney.)

most prominent malpractice attorney, is handling four of the cases against Suburban General and said emphatically that he expected that "it's all going to end up in Common Pleas Court, where the cases should have been in the first place. No one (of the defendants) is going to agree

Polarized connectors —beyond medical infrastructure

Standard header pins are easy to plug something in the wrong way:



Keyed, polarized plugs – only go in one way:

2.50mm JST-XH top-entry (vertical) male PCB connectors

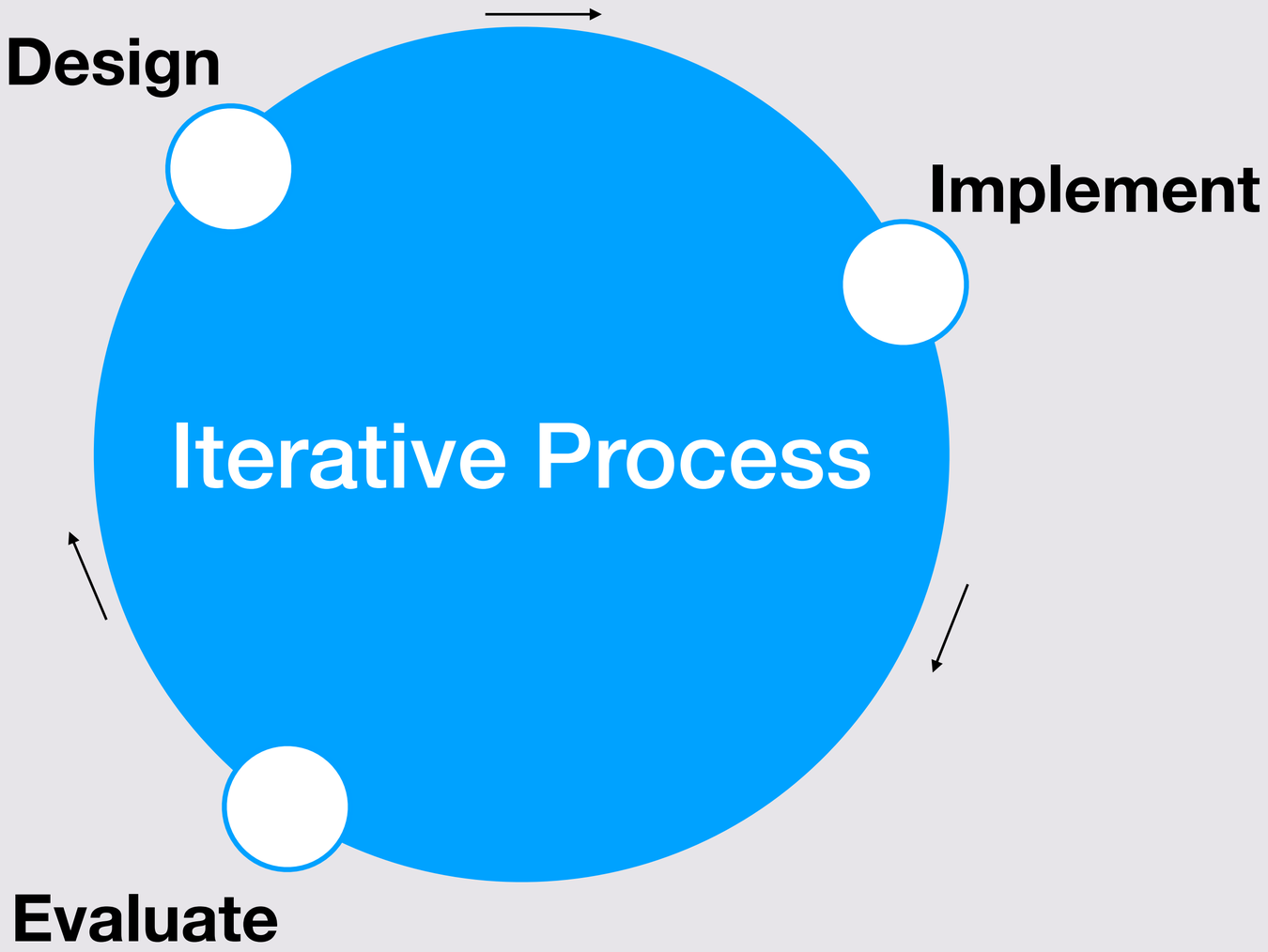
JST RCY connectors

Harvard John A. Paulson
School of Engineering
and Applied Sciences

PL/HCI Seminar (252R/279R)

Types

design & evaluation


Design
Implement
Iterative Process
Evaluate

Types

- “a program p has type T” means that we can tell that p evaluates to an appropriate value, “obviously” — *without* evaluating.
- 1 has type Int, 1+2 has type Int, 100! has type Int.
- This pipe is for oxygen.

Case Study Today

- **Java** is a mainstream and widely studied OO language.
- **Scala** is a language that fuses OO and FP.
- **DOT** is a type-theoretic foundation for Scala:
  - simplify Scala's type system by desugaring into DOT
  - simplify type inference by relying on DOT

Some Papers for Today

- WadlerFest’16 *The Essence of DOT*
  by Amin & Grütter & Odersky & Stucki & Rompf
- OOPSLA’16 *Type Soundness for DOT* by Rompf & Amin
- OOPSLA’16 *Java and Scala’s Type Systems are Unsound: The Existential Crisis of Null Pointers* by Amin & Tate

in Java

```
class Pipe<T> {}
class Source<T> {}
class Assembly<T> {
  public Pipe<T> pipe;
  public Source<T> source; }
class O2 {}
class NO2 {}
public class pipes {
  public static void main(String[] args) {
    Assembly<O2> o2 = new Assembly<O2>();
    o2.pipe = new Pipe<O2>();
    o2.source = new Source<O2>();
    o2.source = new Source<NO2>();
    // error: incompatible types:
    // Source<NO2> cannot be converted to Source<O2>
}}
```

in Scala

```
class Pipe { type T }
class Source { type T }
class Assembly { self =>
  type T;
  var pipe: Pipe { type T = self.T };
  var source: Source { type T = self.T } }
class O2
class N20
object pipes extends App {
  val o2 = new Assembly { type T = O2; }
  o2.pipe = new Pipe { type T = O2; }
  o2.source = new Source { type T = O2; }
  o2.source = new Source { type T = N20; }
}
```

in Scala

```
o2.source = new Source { type T = N2O; }
// error: type mismatch
// found   : Source{type T = N2O}
// required: Source{type T = o2.T}
//    (which expands to)  Source{type T = O2}
```

Soundness

- “Well-typed programs can’t go wrong.”
- “hello”-1, “hello”.foo(1) goes wrong.
- If we have a pipe for oxygen, then the pipe can only be assembled with a source of oxygen.

Unsoundness in Scala

```
// fits in a tweet

trait A { type L >: Any}
def id1(a: A, x: Any): a.L = x
val p: A { type L <: Nothing } = null
def id2(x: Any): Nothing = id1(p, x)
id2(“oh”)
```

```
class Unsound {
  static class Constrain<A, B extends A> {}
  static class Bind<A> {
    <B extends A>
    A upcast(Constrain<A,B> constrain, B b) {
      return b;
    }
  }
  static <T,U> U coerce(T t) {
    Constrain<U,? super T> constrain = null;
    Bind<U> bind = new Bind<U>();
    return bind.upcast(constrain, t);
  }
  public static void main(String[] args) {
    String zero = Unsound.<Integer,String>coerce(0);
  }
}
```

Unsoundness

- Exception in thread "main" java.lang.ClassCastException: java.lang.Integer cannot be cast to java.lang.String
- http://io.livecode.ch/learn/namin/unsound

Unsound pipes

```
Assembly<O2> o2 = new Assembly<O2>();
o2.pipe = new Pipe<O2>();
o2.source = Unsound.<Source<N2O>,Source<O2>>coerce(
  new Source<N2O>());
```

Dependent Object Types

- Minimal theory that can model
  - type parameterization
  - modules
  - objects and classes
  - subtyping

DOT Types

- ⊤
- ⊥
- T ∧ T
- T ∨ T
- L : S..U
- m(x : S) : U
- x.L
- {z ⇒ T}

DOT Types

- ⊤ (top)
- ⊥ (bottom)
- T ∧ T (intersection)
- T ∨ T (union)
- L : S..U (type member)
- m(x : S) : U (method member)
- x.L (type selection)
- {z ⇒ T} (recursive type)

DOT Types

- ⊤ (top)
- ⊥ (bottom)
- T ∧ T (intersection)
- T ∨ T (union)
- L : S..U (type member)
- m(x : S) : U (method member)
- x.L (type selection)
- {z ⇒ T} (recursive type)

(subtyping lattice)

…

…

…

(structural member types)

…

(path-dependent types)

(object types)

Subtyping Lattice

- A lattice has a greatest and lowest type, and for any two types, a least upper bound and greatest lower bound.
- Type inference needs GLB and LUB. e.g. if expression.
- In DOT, GLB = intersection, LUB = union. Well-formed by construction.

Structural Member Types

- Method members.
- By analogy, type members.
- Via intersection, DOT has structural record types.
  (m1(x : S1) : U1) & (m2(x : S2) : U2)

Path-Dependent Types

- Because DOT has type members, it also has an “elimination rule” for them, type selection. If an object o has a type member L, then the type selection o.L is a type, a path-dependent type.
- Type members are defined by a lower bound and an upper bound. Enables translucency.

Object Types

- Recursive self type.
- Objects with recursive self
  $\{z \Rightarrow (L: \bot..\top \;\&\; (m1(x : z.L):z.L) \;\&\; (m2(x:\top):z.L)\}$
- Nominality, through a lower bound of bottom.

a DOT type

```
{ p =>
  type Pipe     : ⊥ .. { type T: ⊥ .. ⊤ }
  type Source   : ⊥ .. { type T: ⊥ .. ⊤ }
  type Assembly : ⊥ .. { z ⇒
    type T: ⊥ .. ⊤
    setPipe  (x: p.Pipe   ∧ { type T: z.T .. z.T }): ⊤
    setSource(x: p.Source ∧ { type T: z.T .. z.T}): ⊤
  }
  type O2: ⊥ .. ⊤
  type N2O: ⊥ .. ⊤
  newAssembly(x: {type T: ⊥..⊤}): z.Assembly ∧ {type T = x.T}
  newPipe    (x: {type T: ⊥..⊤}): z.Pipe     ∧ {type T = x.T}
  newSource  (x: {type T: ⊥..⊤}): z.Source   ∧ {type T = x.T}
}
```

in DOT terms

```
let o2 = p.newAssembly(new {type = p.O2}) in

o2.setPipe  (p.newPipe(new {type = p.O2}));

o2.setSource(p.newPipe(new {type = p.O2}));

o2.setSource(p.newPipe(new {type = p.N2O}));
```

Semantic Intuition

$$\frac{\Gamma \vdash x : (L : S..U)}{\Gamma \vdash S <: x.L <: U}$$

Trouble 1
User-Definable Subtyping Theories

In DOT, the subtyping relation is given in part by user-definable definitions

type T >: S <: U
This makes T a supertype of S and a subtype of U.
By transitivity, S <: U.

So the type definition above proves a subtype relationship which was potentially not provable before.

Bad Bounds

What if the bounds are non-sensical?

type T >: ⊤ <: ⊥
By the same argument as before, this implies that

⊤ <: ⊥
Any <: Nothing *// in Scala*

Once we have that, again by transitivity we get S <: T for arbitrary S and T.
That is the subtyping relation collapses to a point.

Resolution

Evaluation

- PL evaluation of type systems:
  - soundness
  - decidability
  - optional? prescriptive or descriptive?
  - verbosity? type inference.
  - expressivity? powerful orthogonal concepts.
  - predictability? uniqueness of typing.

Evaluation

- HCI evaluation of type systems:
  - What is the user experience of types?
  - How learnable is the type system?
  - Once learned, how powerful is the language?
  - How consistent is it with expectations based on other programming and/or life experience?

Languages vs Users

Group Projects

- Systems HCI requiring heavy-duty PL
  - Humans modifying DSLs for PBD (programming by demonstration)
  - Examplore with interactively defined templates
- Generic human-centered PL
  - Pick language feature, design it in a human-friendly way
  - Pick a language, describe how—and to what extent—its features are being used in the wild
- Usable + X (PL technique)
  - Usable Generative Programming
  - Usable Probabilistic Programming
  - Usable Type System / Verification
  - Usable Synthesis
    - inductive bias alignment between human and machine
    - ranking function improvements
    - DSL improvements
    - expressing constraints on intermediate states, i.e., equivalence values or types

Thank you!

Evaluation

- PL evaluation of type systems
  additional mentioned in discussions
  - complexity
  - completeness (of algorithm wrt to formalism)
  - error handling

Modularity in Java?

- Define an interface, which says: we have some type ‘Key' and some method ‘make’, which takes a ‘String’ and returns a ‘Key’.
- Implement this interface by a class, where type ‘Key’ is type ‘int’ and ‘make’ returns the ‘hashCode’ of the argument.
- Implement as a separate library, a method to ‘map’ the ‘make’ over a list of ‘String’s.

Modularity in OCaml (1)

```
module type GEN = sig
  type key
  val make : string -> key
end;;

module HashGen : GEN = struct
  type key = int
  let make = Hashtbl.hash
end;;
```

Modularity in OCaml (2)

```
module MakeGenLib (Gen: GEN) = struct
  let mapKeys = List.map Gen.make
end;;

module HashGenLib = MakeGenLib(HashGen);;

let ex1 = HashGenLib.mapKeys ["Hello"; “World"];;
(* ex1 : HashGen.key list *)
```

Modularity in Scala

```
trait Gen {
  type Key
  def make(data: String): Key
}

object hashGen extends Gen {
  type Key = Int
  def make(s: String) = s.hashCode
}

def mapKeys(g: Gen, ss: List[String]): List[g.Key] =
  ss.map(g.make)
```

Translucency

$$\frac{\Gamma \vdash x : (L : S..U)}{\Gamma \vdash S <: x.L <: U}$$

```
val abstracted:  Gen { type Key }       = hashGen
val transparent: Gen { type Key = Int } = hashGen

val upperBounded: Gen { type Key <: Int } = hashGen
val lowerBounded: Gen { type Key >: Int } = hashGen
(1: lowerBounded.Key)
(upperBounded.make(“a"): Int)
```

Trouble 2
Type Abstraction vs Type Preservation

```
trait Brand {
  type Hidden
  def pack(x: Int): Hidden
  def unpack(x: Hidden): Int
}
val brand: Brand = new Brand {
  type Hidden = Int
  def pack(x: Int): Hidden = x
  def unpack(x: Hidden): Int = x
}
brand.unpack(brand.pack(7)) // ok
brand.unpack(7) // not ok – but occurs during red.!
```