CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 18: Board RE and circuit edits

Actual board RE

- We talked about components last time.
- Now it's time to cover the board itself.

Typical length scales

- Board dimensions: 5 mm to 500 mm
- Board thickness: 0.1 mm to 3mm
- Copper thickness: 15 µm to 700 µm
- Plating thickness: 250 nm - 40 µm
- Solder mask thickness: 10 to 50 µm
- Copper width: 75 µm - 10 mm

PCB manufacture

- Drill holes in substrate
- Pattern copper
- Stack layers if doing multilayer PCB
- Plate holes
- Soldermask
- Surface plating

Substrates

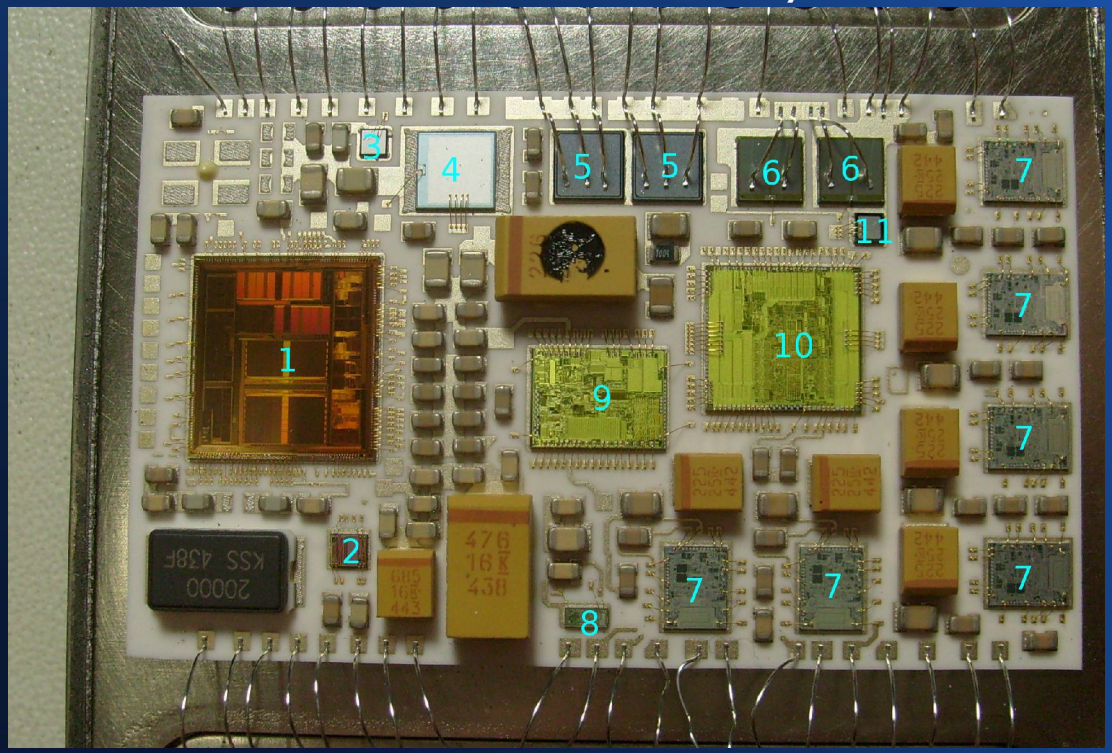
- Provides mechanical support to conductors and components
- Typically used as ILD (some exceptions)

FR-4

- Woven fiberglass cloth in epoxy matrix

Ceramics

- Alumina is typical
- Harsh environments, RF



Esoteric substrates

- Metal
  - Entire PCB is a giant heatsink
  - Typically single-layer power circuits
- Soft plastics
  - Teflon (RF)
  - Polyimide (flex circuits)

Subtractive process

- Glue copper foil to substrate
- Lithography on surface
- Etch away unwanted material
- Wastes lots of copper!

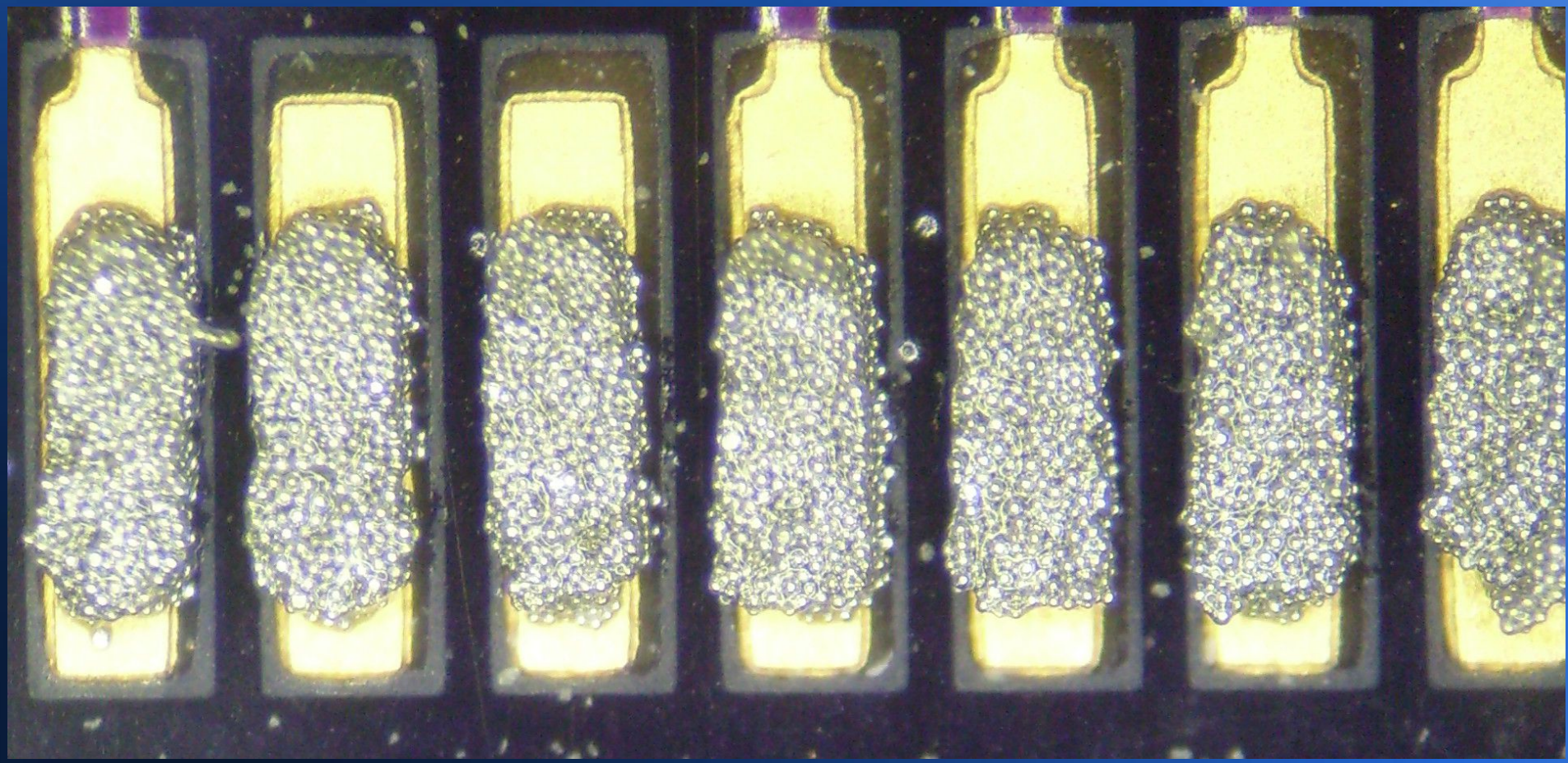
Semi-additive process

- Glue very thin copper foil to substrate
- Lithography with *negative* of metal pattern
- Electroplate more copper on exposed areas
- Strip mask and etch away extra copper

Soldermask

- Polymer layer over copper and substrate
- Provides mechanical protection to traces
- Electrical insulator
- Causes solder to bead up
  - Reduces risk of shorts during assembly
- Typically negative-acting photosensitive film

Soldermask between pasted pads



Via plating

- Typically done before final copper etch
  - All vias and nets are electrically connected
- Litho to expose vias and mask rest of board
- Electroless activator plating (PdCl etc)
- Electroplate copper over activator
- Strip photoresist

Pad plating

- Bare copper corrodes and won't solder reliably
- Exposed pads are typically covered
  - HASL (solder plating)
  - ENIG (gold over nickel)
  - Immersion silver
  - OSP (organic film)

Multilayer boards

- Boards with >2 layers can't be done in one step
- Start with a rigid core and copper on each side
- Add “prepreg” (fiberglass + uncured epoxy)
- Apply heat+pressure to stick together and cure
- Laminate more copper foil
- Drill and plate holes
- Outer layer patterning, soldermask, plating

Reverse engineering

- Ok, we know how boards are made.
- How do we take them apart?
- Key data needed is connectivity between pads

Techniques for netlist extraction

- Optical
  - Visible
  - X-ray
- Electrical

Visible-light imaging

- Photograph board at each layer
- Deprocess to reveal next layer
- Destructive, but straightforward

X-ray imaging

- High-resolution 3D X-ray systems are used in industry for QA
- These same systems can be used to trace out internal nets without deprocessing
- Requires much more expensive equipment
- Components may occlude parts of circuit

Electrical tracing

- Land probes on pads that you think connect
- Bruteforce the netlist by continuity testing
- Nondestructive
- Can be done on small scale with just a DMM
- Hard to scale up to all of a large design

Electrical tracing

- Main use cases
  - Simple designs with only a few pads
  - Checking if some pin is brought out to a header or not
  - Confirming guesses of connectivity
- Can be automated with bed-of-nails or flying-probe test systems, but still $O(N^2)$ scaling

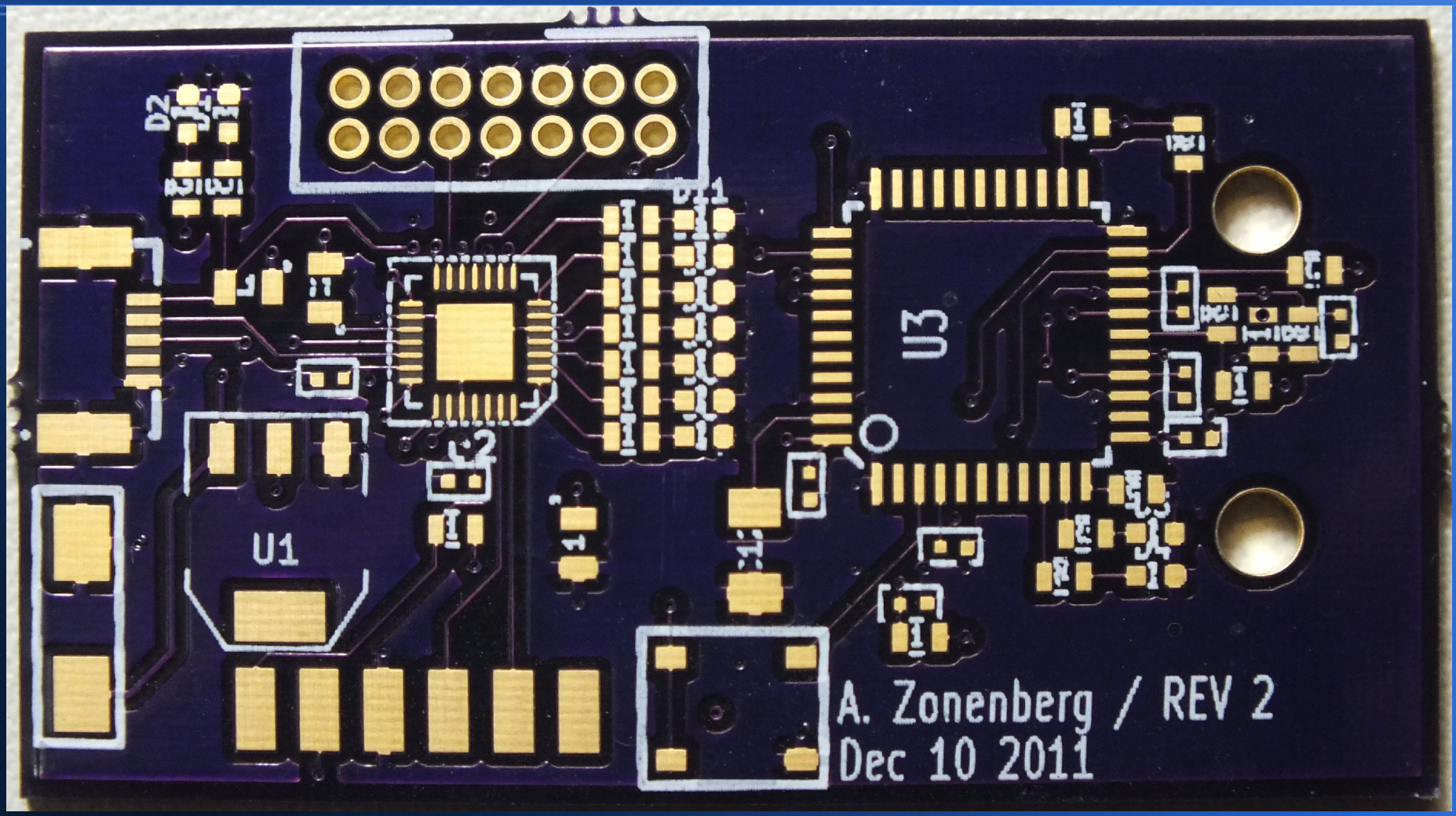
Deprocessing techniques

- Mechanical
- Chemical

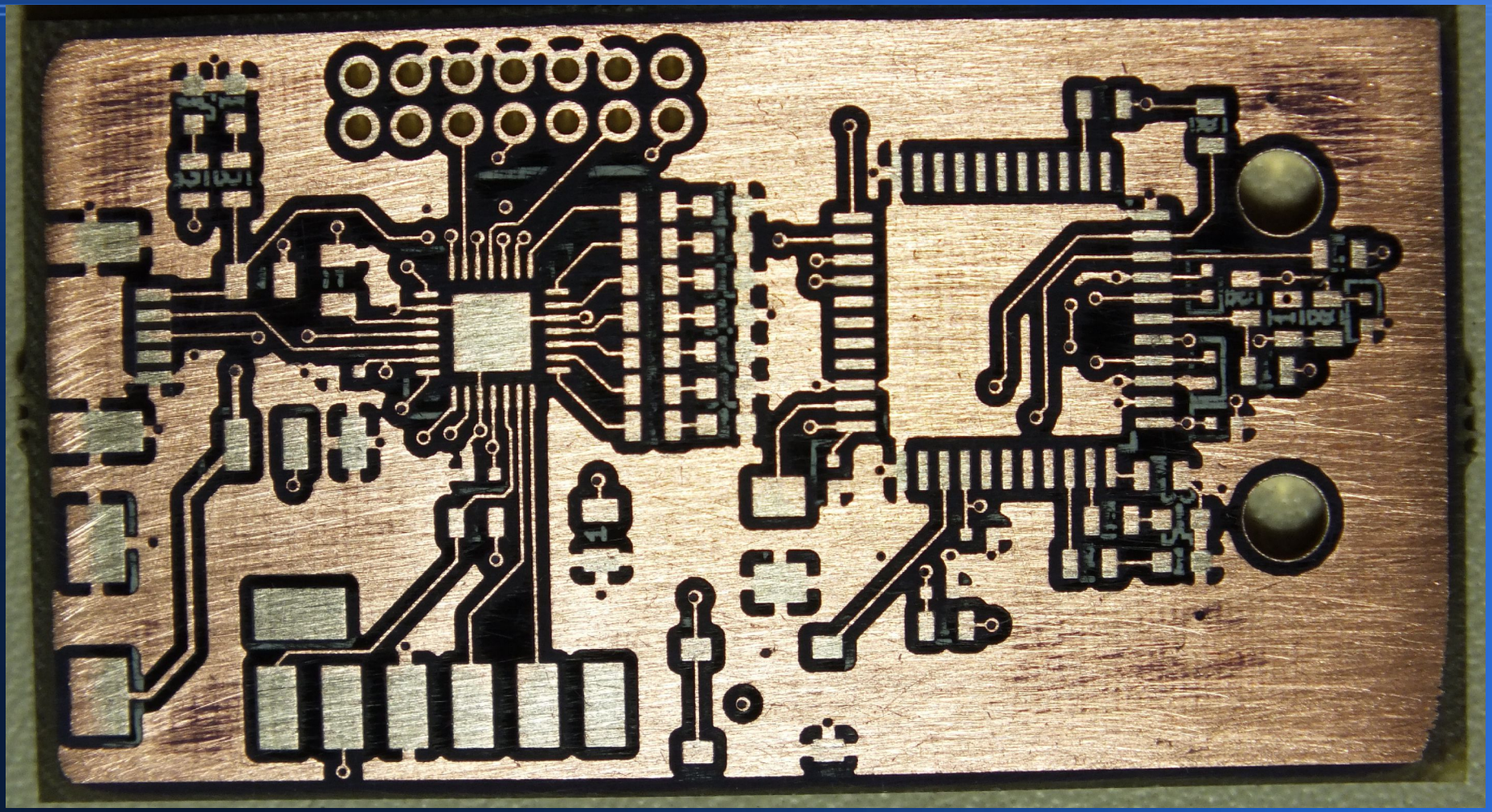
Mechanical deprocessing

- Same basic idea as CMP for IC delayering
- But looser tolerances, typically no chem action
- Can use off-the-shelf sandpaper

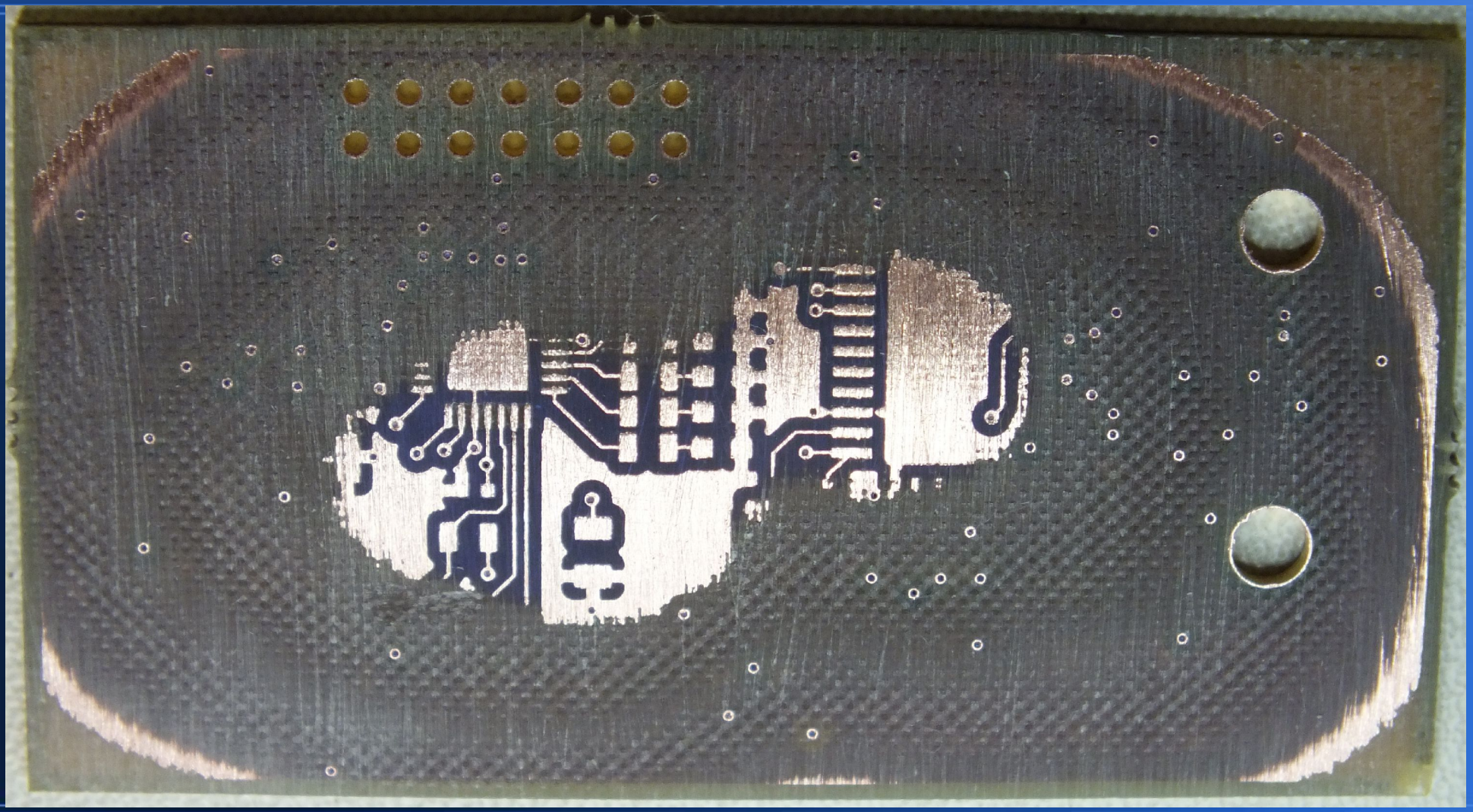
Mechanical deprocessing



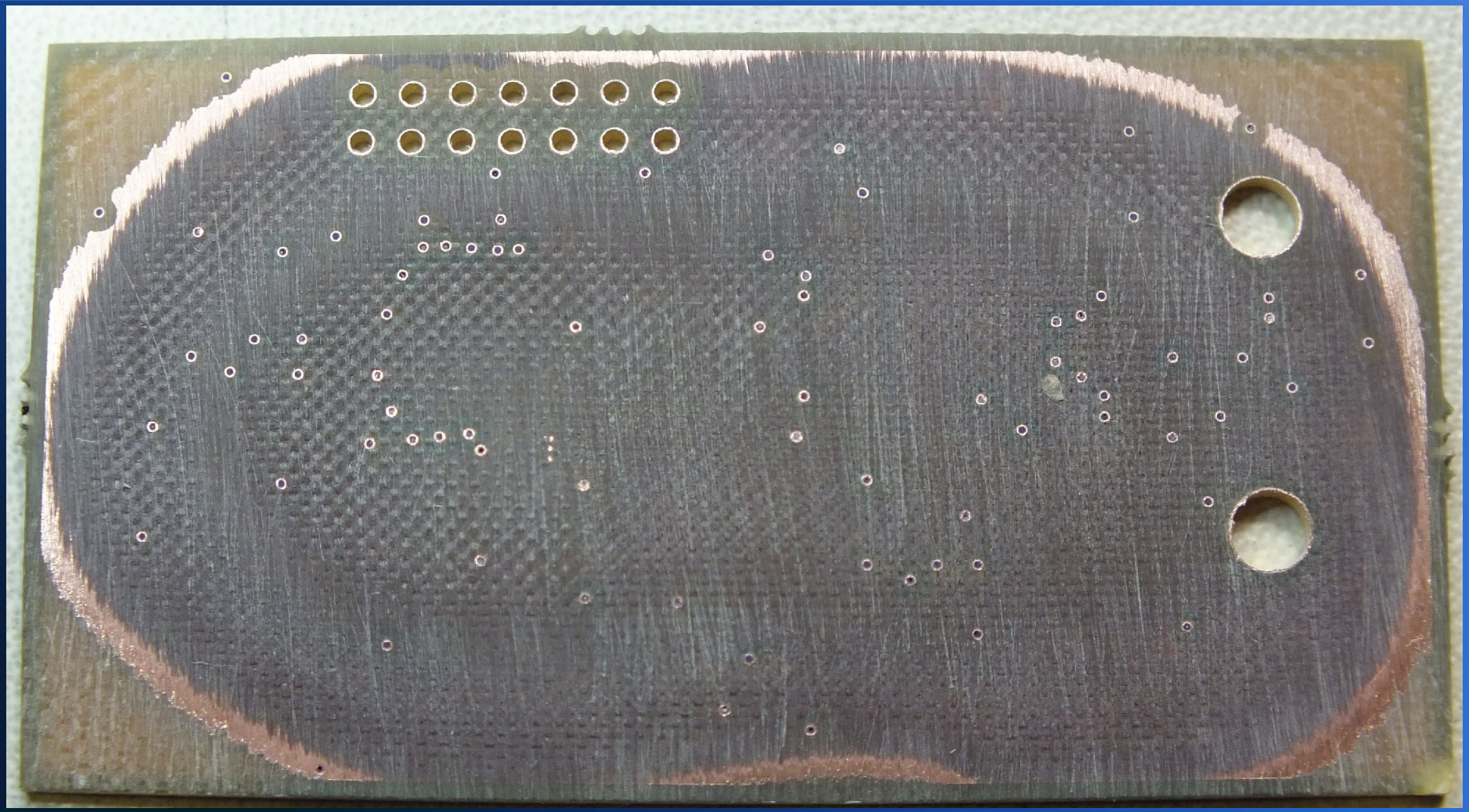
Mechanical deprocessing



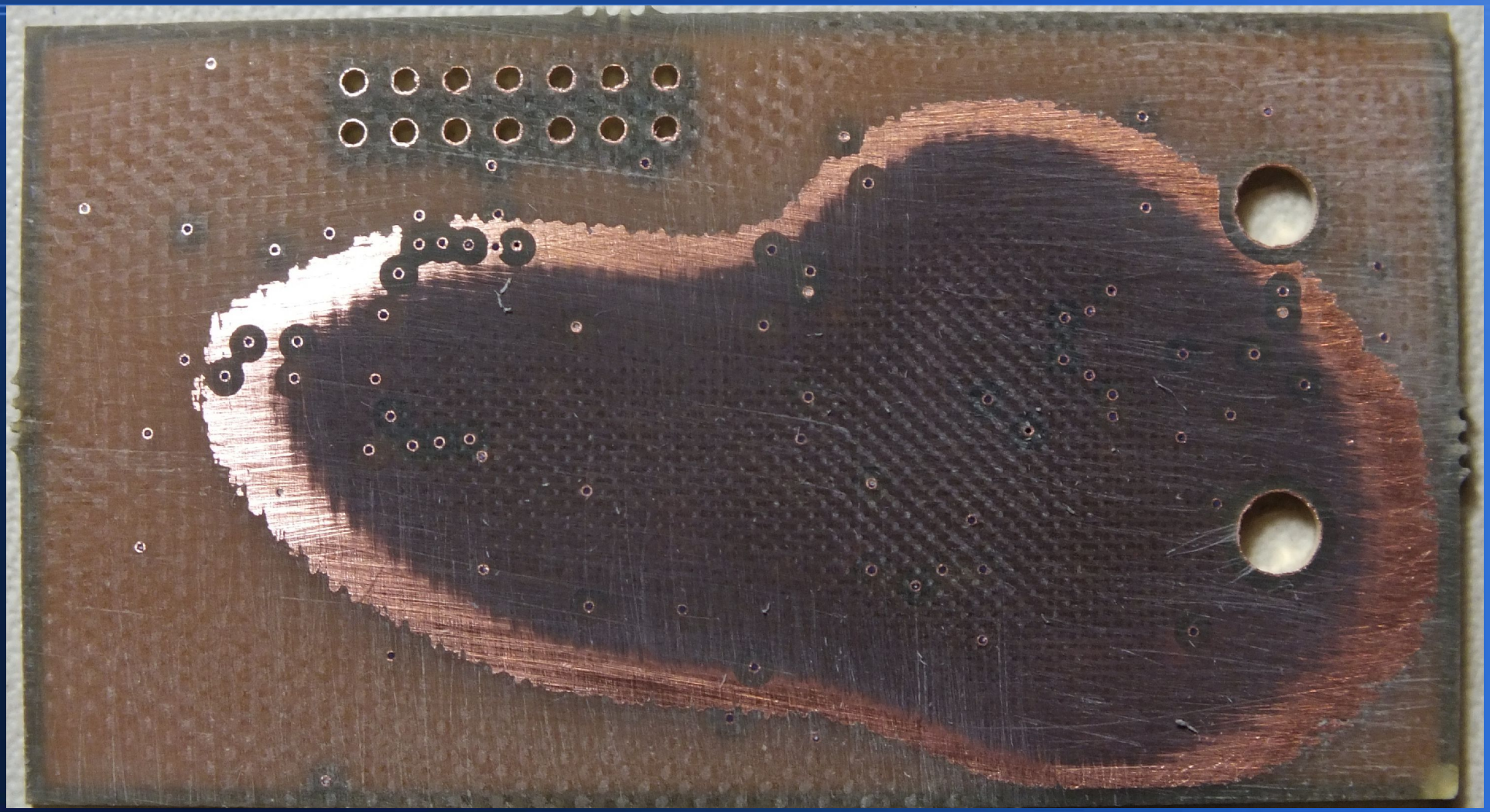
Mechanical deprocessing



Mechanical deprocessing



Mechanical deprocessing



Edge effect

- Analogous to phenomenon seen with CMP
- Same causes
- Solution is the same - sacrificial PCBs

Chemical deprocessing

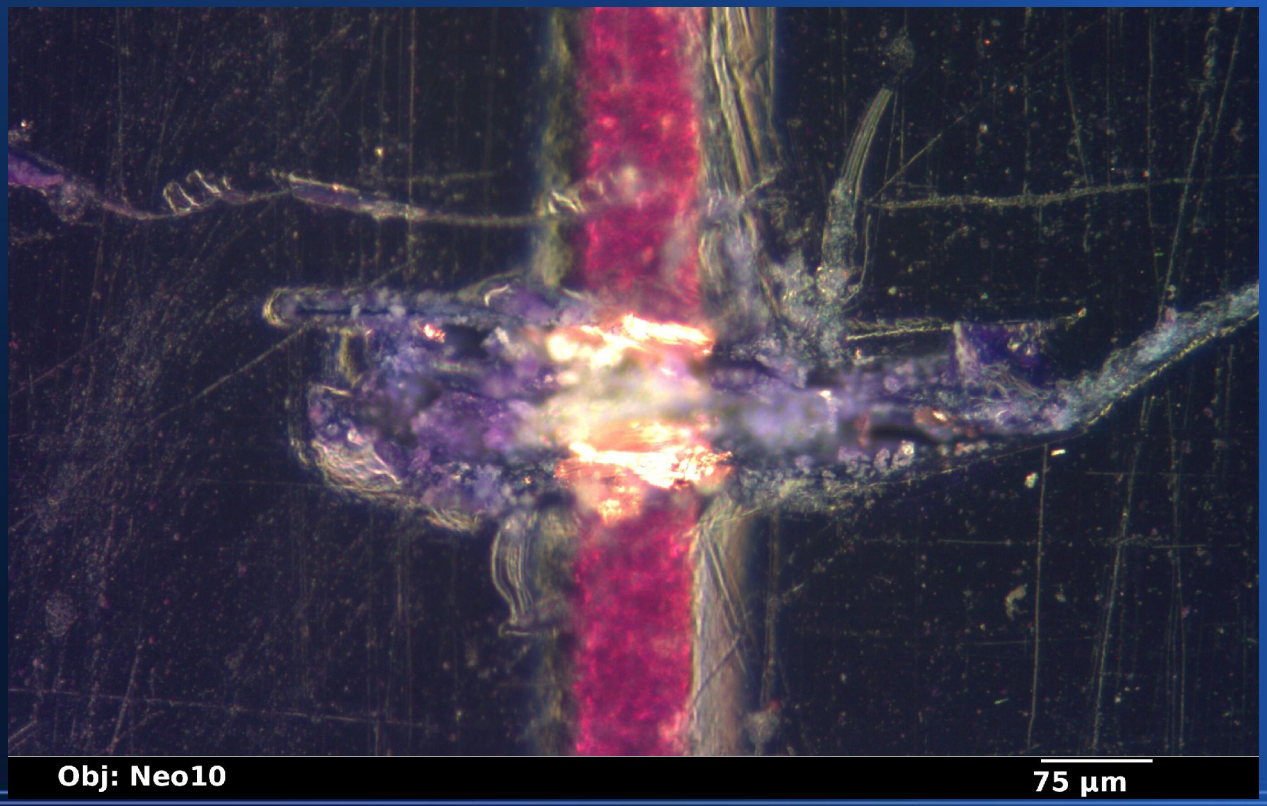
- Can use sulfuric/nitric acids to eat epoxy out from around the glass
- Normally impractical for a large PCB - mechanical techniques tend to give better results

PCB circuit edits

- Standard PCB rework techniques, but used to hack the board rather than fix it ;)
  - Trace cuts
  - Adding traces
  - Via removal
  - Adding vias
  - Removing components
  - Adding components

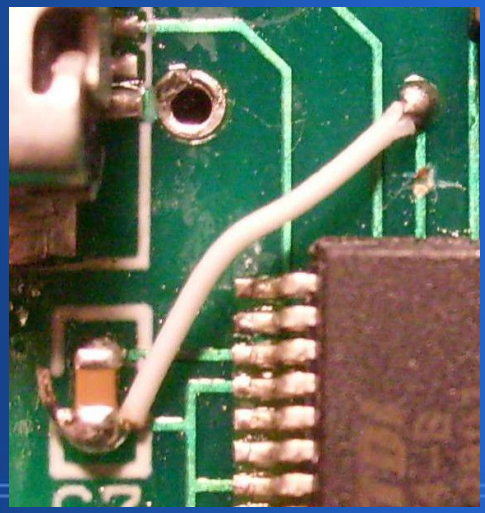
Trace cuts

- Use precision milling tool (similar to dental drill) or scalpel under microscope



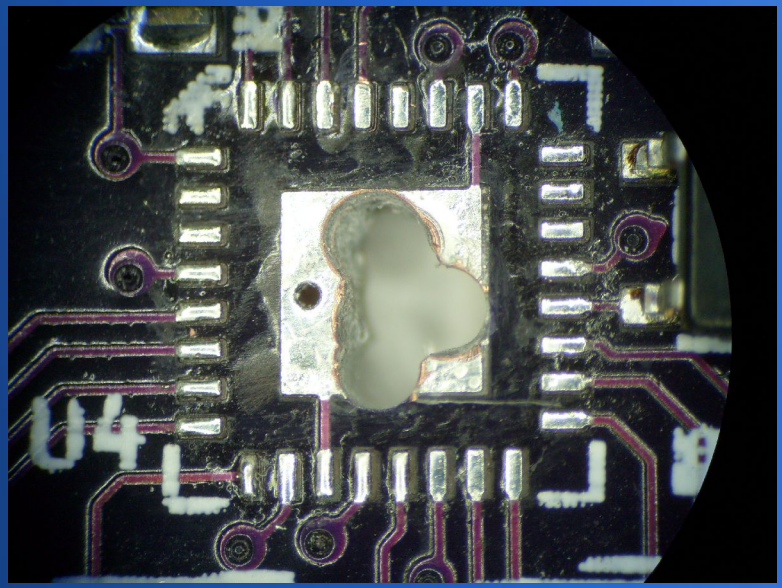
Adding traces

- Use short length of narrow-gauge copper wire
- Solder to each end and tape down
- Wire-wrap wire is common and cheap
- Can also get custom-made square wires with glue on underside (sold under Circuit Tracks brand name by circuitmedic and others)



Via removal

- Find drill bit slightly larger than hole
- Drill out plating on hole sidewall
- Example shown is overkill, but saved the board (no smaller bits were handy!)



Via insertion

- Fairly easy for 2-layer boards
- Find the appropriate area
- Drill hole
- Run wire through hole and solder to each side

Via insertion

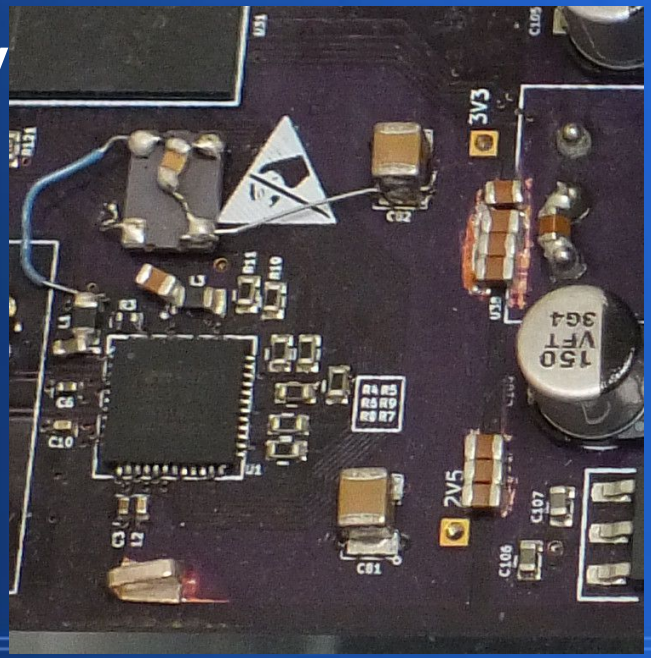
- Creating vias in multilayer boards is harder
- Mill hole through outer layers to expose inner copper
- Solder wire to inner-layer trace/plane
- Repeat as needed for other end of wire

Removing components

- Heat with hot air rework tool
- Remove part with tweezers

Adding extra components

- Often done “dead bug” style
  - Glue top of component to the board
  - Run wires from leads to destination pads
- Scrape soldermask away as necessary



Questions?

- TA: Andrew Zonenberg <azonenberg@drawersteak.com>
- Image credit: Some images CC-BY from:
  - John McMaster <JohnDMcMaster@gmail.com>