data-ppf.github.io mar 3, 2020

lecture 7 of 14: WWII, dawn of digital computation

chris wiggins + matt jones, Columbia

logistics/housecleaning

- see FAQ for new schedule for HW, etc

logistics/housecleaning

- see FAQ for new schedule for HW, etc
- Op-Ed assigned already via `#general` in Slack

student reactions

student reactions: some data on people, ideas, things

```
124 Turing
109 women
44 Mcgrayne
41 labor
39 Bayesian
12 Hicks
4 wrens
4 Shannon
```

student reactions: vs "last week"

wartime...contrasts with the feuding between Neyman and Fisher that we saw last week

Unlike last week's readings...these readings reminded me once again of data's tangible potential

Whereas last week's readings were enmeshed in the theoretical...

I was surprised at the leap from the statistical and academic debate we had last week between Fisher and Neyman-Pearson to the dearth of statistics...

...shift away from last week's squabbles between Fisher and Neyman...

After last week's petty math-battle readings, it was refreshing to read...

Moreover, after last week's battle of the statisticians, it was inspiring to see...

student reactions: "sad"/upsetting

it saddened me [that Bletchley workers were] unable to even discuss their work

it deeply saddens me that . . . governments . . . did not allow women to reach their full potential or, after the war, ban gay men like Turing from continuing their work

It is also saddening to see the perception of [women's] lower status labor internalized.

It makes me sad to consider the loss to society due to his death

it's saddening and frustrating that women were continually left out of the picture and how, even today, the names of those same women are still largely forgotten

the harassment [women] received behind the scenes was simply saddening to read

Lastly, Turing's defeat and eventual death is incredibly upsetting to me and makes me question what other influential individuals have been silenced and erased from

student reactions: context on "stereotype"

the Mar Hicks piece broke through the stereotypes of computing as a male dominated field

% Of Women Majors, By Field

Legend: Medical School, Law School, Physical Sciences, Computer science
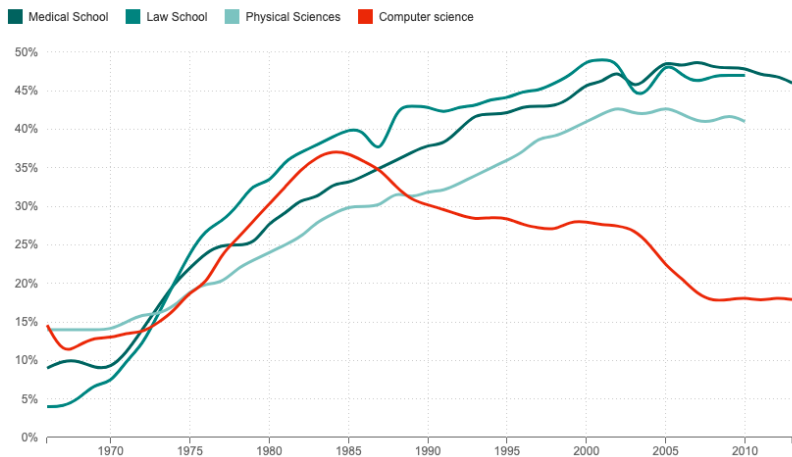
Source: National Science Foundation, American Bar Association, American Association of Medical Colleges
Credit: Quoctrung Bui/NPR

Figure 1: When Women Stopped Coding, Planet Money, October 21, 2014

themes for today

- hardware, labor, power

themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far

themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM, content moderation. . .)

themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM, content moderation...)
  - now labor becomes visible, as computation is born

themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM, content moderation...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value

themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM, content moderation...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)

themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM, content moderation...)
  - now labor becomes visible, as computation is born
  - immediately, the gendering of labor happens, segregating task + value
  - "the gendered nature of technical skill [and] of labor" (-Abbate)
  - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power

themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM, content moderation. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones

themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM, content moderation. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task $+$ value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)

themes for today

- ▶ hardware, labor, power
    - ▶ the labor behind 'data' has been absent so far
    - ▶ (later we'll see labor in collection of data, census, IBM, content moderation. . .)
    - ▶ now labor becomes visible, as computation is born
    - ▶ immediately, the gendering of labor happens, segregating task + value
    - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
    - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
    - ▶ similar valuation of skills (classics, math, engineering, stats)
    - ▶ trading zones

themes for today

- ▶ hardware, labor, power
  - ▶ the labor behind 'data' has been absent so far
  - ▶ (later we'll see labor in collection of data, census, IBM, content moderation...)
  - ▶ now labor becomes visible, as computation is born
  - ▶ immediately, the gendering of labor happens, segregating task + value
  - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
  - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
  - ▶ similar valuation of skills (classics, math, engineering, stats)
  - ▶ trading zones
  - ▶ driving problem is engineering not science

themes for today

- ► hardware, labor, power
    - ► the labor behind 'data' has been absent so far
    - ► (later we'll see labor in collection of data, census, IBM, content moderation...)
    - ► now labor becomes visible, as computation is born
    - ► immediately, the gendering of labor happens, segregating task + value
    - ► "the gendered nature of technical skill [and] of labor" (-Abbate)
    - ► *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ► Bayes and trading zones
    - ► similar valuation of skills (classics, math, engineering, stats)
    - ► trading zones
    - ► driving problem is engineering not science
- ► role of state and power, transfer immediately to corporations

themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM, content moderation. . .)
  - now labor becomes visible, as computation is born
  - immediately, the gendering of labor happens, segregating task + value
  - "the gendered nature of technical skill [and] of labor" (-Abbate)
  - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
  - similar valuation of skills (classics, math, engineering, stats)
  - trading zones
  - driving problem is engineering not science
- role of state and power, transfer immediately to corporations
  - UK: post office

themes for today

- ▶ hardware, labor, power
    - ▶ the labor behind 'data' has been absent so far
    - ▶ (later we'll see labor in collection of data, census, IBM, content moderation. . .)
    - ▶ now labor becomes visible, as computation is born
    - ▶ immediately, the gendering of labor happens, segregating task + value
    - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
    - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
    - ▶ similar valuation of skills (classics, math, engineering, stats)
    - ▶ trading zones
    - ▶ driving problem is engineering not science
- ▶ role of state and power, transfer immediately to corporations
    - ▶ UK: post office
    - ▶ US: telecommunications, NCR, etc. . .

themes for today

- ▶ hardware, labor, power
  - ▶ the labor behind 'data' has been absent so far
  - ▶ (later we'll see labor in collection of data, census, IBM, content moderation. . .)
  - ▶ now labor becomes visible, as computation is born
  - ▶ immediately, the gendering of labor happens, segregating task + value
  - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
  - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
  - ▶ similar valuation of skills (classics, math, engineering, stats)
  - ▶ trading zones
  - ▶ driving problem is engineering not science
- ▶ role of state and power, transfer immediately to corporations
  - ▶ UK: post office
  - ▶ US: telecommunications, NCR, etc. . .
  - ▶ note this is an age *creating* industrial-military complex

themes for today

- ► hardware, labor, power
    - ► the labor behind 'data' has been absent so far
    - ► (later we'll see labor in collection of data, census, IBM, content moderation. . .)
    - ► now labor becomes visible, as computation is born
    - ► immediately, the gendering of labor happens, segregating task + value
    - ► "the gendered nature of technical skill [and] of labor" (-Abbate)
    - ► *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ► Bayes and trading zones
    - ► similar valuation of skills (classics, math, engineering, stats)
    - ► trading zones
    - ► driving problem is engineering not science
- ► role of state and power, transfer immediately to corporations
    - ► UK: post office
    - ► US: telecommunications, NCR, etc. . .
    - ► note this is an age *creating* industrial-military complex
    - ► note this is an age *creating* industrial-military-academic complex

themes for today

- ▶ hardware, labor, power
  - ▶ the labor behind 'data' has been absent so far
  - ▶ (later we'll see labor in collection of data, census, IBM, content moderation...)
  - ▶ now labor becomes visible, as computation is born
  - ▶ immediately, the gendering of labor happens, segregating task + value
  - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
  - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
  - ▶ similar valuation of skills (classics, math, engineering, stats)
  - ▶ trading zones
  - ▶ driving problem is engineering not science
- ▶ role of state and power, transfer immediately to corporations
  - ▶ UK: post office
  - ▶ US: telecommunications, NCR, etc...
  - ▶ note this is an age *creating* industrial-military complex
  - ▶ note this is an age *creating* industrial-military-academic complex
    - ▶ 'secrecy' ties into this power

guiding questions every week:

- Scientific and mathematical development

guiding questions every week:

- Scientific and mathematical development
- Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)

guiding questions every week:

- Scientific and mathematical development
- Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)
- Driving forces: money, prestige, resources, Imperial competition... and "truth!"

guiding questions every week:

- Scientific and mathematical development
- Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)
- Driving forces: money, prestige, resources, Imperial competition... and "truth!"
- how did new capabilities rearrange power? (who can now do what, from what, to whom?) (rights, harms, justice)

context: people, ideas, things

historical & social context

- academia: math-fight

historical & social context

- academia: math-fight
- IRL: WWII

historical & social context

- academia: math-fight
- IRL: WWII
- for next weeks:

historical & social context

- academia: math-fight
- IRL: WWII
- for next weeks:
  - computation: "The ENIAC was completed and ran its first program in November 1945—too late to help in the war effort but just in time to influence the postwar computer industry."

historical & social context

- academia: math-fight
- IRL: WWII
- for next weeks:
    - computation: "The ENIAC was completed and ran its first program in November 1945—too late to help in the war effort but just in time to influence the postwar computer industry."
    - industrial data: role of Bell, IBM, NCR, and OSS/NSA

Readings: McGrayne, NSA, Hicks, Hodges,

secondary readings

- Sharon McGrayne

secondary readings

- Sharon McGrayne
- Mar Hicks

secondary readings

- Sharon McGrayne
- Mar Hicks
- (bonus: Janet Abbate)

secondary readings

- Sharon McGrayne
- Mar Hicks
- (bonus: Janet Abbate)
  - "British Post Office electrical engineer Tommy Flowers"

secondary readings

- Sharon McGrayne
- Mar Hicks
- (bonus: Janet Abbate)
  - "British Post Office electrical engineer Tommy Flowers"
- Turing bio from Hodges

secondary readings

- Sharon McGrayne
- Mar Hicks
- (bonus: Janet Abbate)
  - "British Post Office electrical engineer Tommy Flowers"
- Turing bio from Hodges
- (bonus: NSA history)

secondary readings

- Sharon McGrayne
- Mar Hicks
- (bonus: Janet Abbate)
  - "British Post Office electrical engineer Tommy Flowers"
- Turing bio from Hodges
- (bonus: NSA history)
- (bonus: Turing on Turing)

McGrayne on Bayes

By 1939 Bayes' rule was virtually <u>taboo</u>, dead and buried as far as statisticians in the know were concerned. A disturbing question remained, though. How could wartime leaders make the best possible life-and-death decisions swiftly, without waiting for complete information? In deepest secrecy some of the greatest mathematical minds of the century would contribute to rethinking Bayes' role during the uncertain years ahead.

Figure 2: trading zone (1/2)

McGrayne on Bayes

Strangely enough, the Poles were the first to think otherwise. A few intelligence officers in Poland, sandwiched as they were between Germany and Russia, realized a full decade before the start of the Second World War that mathematics could make eavesdropping on their rapacious neighbors quite informative. The First World War had made the need for machines to encode radio messages painfully obvious. When an alphabet-scrambling machine was exhibited at an international trade show in 1923, Germany bought some and began introducing complexities to make their codes more secure. The machines were named Enigma.

Figure 3: labor, engineering, innovation

McGrayne on Bayes

Unlike the Poles, the British agency charged with cracking German military codes and ciphers clung to the tradition that decryption was a job for gentlemen with linguistic skills. Instead of hiring mathematicians, the Government Code and Cypher School (GC&CS) employed art historians, scholars of ancient Greek and medieval German, crossword puzzlers, and chess players. Mathematicians were regarded as "strange fellows."[2]

The British government and educational systems treated applied mathematics and statistics as largely irrelevant to practical problems. Well-to-do boys in English boarding schools learned Greek and Latin but not science and engineering, which were associated with low-class trade. Britain had no elite engineering schools like MIT or the École Polytechnique. Two years into the war, when government officials went to Oxford to recruit men proficient in both mathematics and modern languages, they found only an undergraduate mathematics major teaching himself beginning German. The government did not even plan to exempt mathematicians from combat. Knowing that their skills would be needed eventually, mathematicians quietly spread word to their colleagues to register with the government as physicists because they at least were considered vital to the nation's defense.

McGrayne on Bayes

With applied mathematicians and statisticians in short supply, wartime data were often analyzed not by statisticians but by actuaries, biologists, physicists, and pure mathematicians—few of whom knew that, as far as sophisticated statistics was concerned, Bayes' rule was unscientific. Their ignorance proved fortunate.

Figure 5: trading zone (2/2)

McGrayne on Bayes

In a fundamental breakthrough, Turing realized he could not systematize his hunches or compare their probabilities without a unit of measurement. He named his unit a ban for Banburismus and defined it as "about the smallest change in weight of evidence that is directly perceptible to human intuition."[13] One ban represented odds of 10 to 1 in favor of a guess, but Turing normally dealt with much smaller quantities, decibans and even centibans. The ban was basically the same as the bit, the measure of information Claude Shannon discovered by using Bayes' rule at roughly the same time at Bell Telephone Laboratories. Turing's measure of belief, the ban, and its supporting mathematical framework have been called his greatest intellectual contribution to Britain's defense.

named
by
Tukey

Figure 6: technology and corporate resources

McGrayne on Bayes

In operation, Banburismus used 5- or 6-foot-long strips of thin cardboard printed in Banbury. Decoders look for repetitions and coincidences, so Wrens, technicians from the Women's Royal Naval Service, punched each intercepted message by hand, letter by letter, into a Banbury sheet. Then they slipped one strip on top of others so that any two messages could be compared. When enough letter holes showed through both Banburies, the number of repeats was recorded.

Figure 7: labor, unseen and/or erased

McGrayne on Bayes

> Kolmogorov became the world's authority on probability theory. In 1933 he demonstrated that probability is indeed a branch of mathematics, founded on basic axioms and far removed from its indecorous gambling origins. So fundamental was Kolmogorov's approach that any mathematician, frequentist or Bayesian, could legitimately use probability. Kolmogorov himself espoused the frequentist approach.

Figure 8: 'Russian' mathematics, trading zone

see also "No Bayesians in foxholes" 1997, Breiman

"a strongly anti-Bayesian position which used to be common in statistics" – Gelman

McGrayne on Bayes

Turing spent at least one afternoon in Dayton, where the National Cash Register Company planned to manufacture 336 bombes. He was dismayed to discover that the U.S. Navy was ignoring Banburismus and its ability to economize on bombe usage. The Americans seemed uninterested in the Enigma outside of their obligation to supply bombes for it.

Figure 9: contractor mindset @ NCR

McGrayne on Bayes

Max Newman, formerly Turing's mathematics instructor at Cambridge, wanted to automate the British attack on Tunny-Lorenz's codes, and he, Michie, and Good were already working on new machines to do it. Michie had refined Turingismus, but it soon became obvious that mechanical switches would be far too slow. The process would have to be electronic; engineer Thomas H. Flowers suggested using glass vacuum tubes because they could switch current on and off much faster. With backing from Newman, Flowers built the first Colossus at the Post Office Research Station, which ran Britain's telephone system. Installed at Bletchley Park, Colossus decrypted its first message on February 5, 1944. Flowers's car broke down that day but not his Colossus.

Figure 10: UK 'post' (telecommunications too)

McGrayne on Bayes

By 1945 U.S. cryptanalysts were writing memos to one another about Bayes' theorem. Whether the Americans learned about Bayes from Bletchley Park or discovered its usefulness on their own is not known; 65 years after the war, the British government still refuses to declassify many documents about wartime cryptography. A young American mathematician, Andrew Gleason, who was working on Japanese naval codes and who looked after Turing during his stay in Washington, almost certainly knew about Bayes during the war. He, Good, and Alexander continued to work on top-secret cryptography for decades after the war. Gleason helped establish a postwar

Figure 11: behind the fence; Bayes and data science

mar hicks: gendering labor

> *In Britain, women often built the machines as well. The manufacturing workforce at IBM UK was so feminized that management measured its production in "girl hours" rather than "man hours" into the 1960s.'*

> *The growing popularity of the typewriter in late Victorian offices had helped create an association of automation with feminized labor pools*

> *Throughout the war, supervisors struggled to decide on how much to gender jobs in the midst of crisis; an April 1942 report from Bletchley Park investigated the "number of new posts that can be filled by women" and stated the percentages women should take up for each job class."*

see also code girls

My great sadness is that my beloved husband died in 1975 without knowing what I did in the war.

These extreme security measures continued to influence the historiog- raphy of labor and technology for decades after the war, paradoxically ensuring that British accomplishments went down in history as also-rans in a US-centric story of early electronic computing.

mar hicks: long term impact

Defined by its wartime origins, electronic computing was arguably Britain's most critical twentieth-century project. Hidden, wartime com- puter operators had a growing analogue in peacetime: the "broad base" of the Civil Service's data-processing establishment, which rested on fem- inized and largely ignored classes of machine workers. As a tool in times of stability and peace, not just in times of war, computerization's his- tory is largely a narrative of the expanding reach and power of the data- intensive state.'

Abbate on "Women at the Dawn"

I was a Colossus operator, which we considered to be the crème de la crème. We felt we were "at the sharp end," where there was a great tension and flow of adrenaline . . . operating those incredible machines.

—Jean Beech, Colossus operator[1]

I don't know if you can picture how exciting the ENIAC was to all of us. And we didn't talk socially or any other time about anything else. It was—we discussed it almost all the time.

—Jean Jennings, ENIAC programmer[2]

Figure 12: motivation: in their own words

Abbate on "Women at the Dawn"

Computer Work and the Gendered Division of Labor

By the time I reached my third year of college, I started looking around for some type of occupation that could use a math major. I didn't want teaching. Insurance companies' actuarial positions required a master's degree (and they seldom hired women, I later found out). . . . Just after graduation, I happened to see an ad in the daily paper. The Army was looking for women with a degree in mathematics—right here in Philadelphia.

—Kay McNulty, ENIAC programmer[19]

Figure 13: 'labor shortage'

manageable for women, assuring them, "If you've used an electric mixer in your kitchen, you can learn to run a drill press."[23] At the same time,

Figure 14: forced models of labor

Abbate on "Women at the Dawn"

In the scientific world, women had been employed in large numbers to do calculations by hand. These human computers generally, although not always, had some training in mathematics, and it was from the ranks of such mathematically trained women that the ENIAC project drew its first corps of programmers. However, even women with college degrees were relegated to subprofessional job classifications. As Kay McNulty recalled, "The girls were told that only 'men' could get professional ratings."[25] The ENIAC programmers were not promoted from computer to mathematician—a professional rating—until January 1946.[26]

Figure 15: prior labor dynamics, and power dynamics

Abbate on "Women at the Dawn"

computer. Dividing the task this way was meant to conserve the scarce labor of trained mathematicians. It also reproduced a gender hierarchy: all of the cryptographers working with Colossus were men, and all of the operators were women.[27] As B. Jack Copeland notes in his history

Figure 16: org chart as weapon of oppression

in favor of original thought and good work."[31] While men's supposedly more creative work excused them from military exercises, Colossus operator Catherine Caughey described how the Wrens were forced to do drills and marches after working all night on the machine: "They made us do an hour's squad-drill on the gravel in front of the Abbey every morning. . . . We were all being killed by the constant changes of shift. Church Parade on a Sunday was compulsory. On my first Sunday, when I was on nights, I had to assemble with the others. We had to march two miles each way to the village church, along an icy road."[32] The arduous and seemingly unnecessary demands placed on the Colossus operators reveal their superiors' unspoken presumption that women's work is by nature mundane and does not require one's full energies. Such gender stereotyping can be destructively self-fulfilling. With their work seen as less important, women are loaded down with extra chores such as military drills (or in the present day, housework or low-level administrative tasks). These burdens, in turn, make it harder for women to perform up to their potential, reinforcing the idea that they are less capable than men. In the Bletchley

Figure 17: 'destructively self-fulfilling'

Abbate on "Women at the Dawn"

Occasionally, the six of us programmers all got together to discuss how we thought the machine worked. If this sounds haphazard, it was. The biggest advantage of learning the ENIAC from the diagrams was that we began to understand what it could and what it could not do. As a result we could diagnose troubles almost down to the individual vacuum tube. Since we knew both the application and the machine, we learned to diagnose troubles as well as, if not better than, the engineer.

—Jean Jennings, ENIAC programmer[36]

Figure 18: depth of understanding

Initial Assumptions about Computing Work

The selection criteria and job training for Colossus and ENIAC indicate that these tasks were believed to require at least some mathematical ability and that the best available female workers were assigned to the computers. Wrens were placed in Max Newman's mechanical codebreaking section based on an eclectic mix of technical and social qualifications: "Wrens were chosen by interview. . . . No fixed qualifications were required, though a pass in mathematics in School Certificate or apparently 'good social recommendations' was normally considered essential. . . . None had studied mathematics at the university."[37] Newman gave prospective operators a two-week course covering binary math, the teletype alphabet code, and machine operation, after which they were given a written exam. Those with the highest scores were given the most challenging assignments, including Colossus.[38] The first Colossus operators were presumably trained by Newman himself to use the machines, but after that experienced operators took on the responsibility of training new recruits, adding another dimension to their duties.

Qualifications were higher for ENIAC. The six programmers all had

Abbate on "Women at the Dawn"

To be a successful Colossus operator therefore required physical endurance, mechanical aptitude, attention to detail, and the ability to memorize codes and do mental arithmetic. Female operators were also entrusted with a certain amount of initiative. They did some runs without supervision, evaluating the results to determine if the correct wheel setting had been found.[50] They were also trained by the engineers to do routine testing of the machines, and they solved some minor mechanical problems,

Figure 19: skill mix

cords, Ruth Lichterman was quick to correct him.

Q: When you say you programmed the machine, did that mean physically that you took these plugs from one place and plugged them into another place?
[Ruth Lichterman]: Well, now, program means several things. . . . You got a problem, and you started with pencil and paper, and you decided how you were going to do this problem and which numbers went where. . . . [Y]ou drew a diagram of all this stuff and then you actually went on the machine, and we call that "plugging in" rather than "program."[59]

Figure 20: programming and plugging

Abbate on "Women at the Dawn"

Constructing Opportunities for Women in Computing at War's End

We had to sign the Secrets Act when we left, and we had to take all these machines down. My parents never knew what I did, and neither did my husband. I never told anybody at all. None of us ever did.

—Eleanor Ireland, Colossus operator[67]

Figure 21: secrecy

Abbate on "Women at the Dawn"

One common experience for the Colossus and ENIAC women was that neither group received public recognition for their work, either during the war or for many decades afterward. At Bletchley Park, there was complete secrecy: not even the Wrens' families found out what they had

Figure 22: secrecy and un-history

I wasn't included on any of the pictures of the entire stupid thing." Kay McNulty noted ruefully, "None of us girls were ever introduced [at the press conference]; we were just programmers."[79] It was not until the fiftieth anniversary of the ENIAC that historians rediscovered and began to publicize the ENIAC women's contribution.[80]

Figure 23: erasure

Alan's work on the RCA cipher seemed to show that his method would not work. He joined in the work of the 'cell' on another approach to the problem. Despite the great technical secrecy, there were enough straws in the wind for his colleagues to realise that he was doing other, top-level, work. Thus it was noted that while speaking with H. Nyquist, one of the top Bell consultants working on the X-system, Alan had met William Friedman, who was the chief American cryptanalyst.

Friedmans

Figure 24: William and Elizebeth Friedman

- ▶ couple met under patron wanting to reveal the true Shakespeare

Friedmans

- tiny US crypto community during WW1 and between wars

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes
- help create unified NSA

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes
- help create unified NSA
- push toward project of large supercomputers

primary readings: Turing by Hodges: NYC

> *He went down to New York City, arriving at the Bell Laboratories building on West Street, by the piers, on the afternoon of 19 January 1943. And for two months he soaked himself in the electronic technology of speech encipherment.*

Russell and Einstein, Hardy and Eddington. . . longed to jump out of the system of La Grande Illusion [i.e., were pacifists]. . . In 1933 they had reviled the arms manufacturers above all others. But they were all arms manufacturers now.

Shannon: mathematical theory of crypto/communications

COVER SHEET FOR TECHNICAL MEMORANDA

RESEARCH DEPARTMENT

SUBJECT: A Mathematical Theory of Cryptography - Case 20878 (4)

ROUTING:
1 – H. B-HF-Case Files
2 – CASE FILES
3 – J. W. McRae
4 – L. Espenschied
5 – H. S. Black
6 – F. B. Llewellyn
7 – H. Nyquist
8 – B. M. Oliver
9 – R. K. Potter
10 – C. B. H. Feldman
11 – R. C. Mathes
12 – R. V. L. Hartley
13 – J. R. Pierce
14 – H. W. Bode
15 – R. L. Dietzold
16 – L. A. MacColl
17 – W. A. Shewhart
18 – S. A. Schelkunoff
19 – C. E. Shannon
20 – Dept. 1000 Files

MM – 45-110-92
DATE September 1, 1945
AUTHOR C. E. Shannon
INDEX NO. P 0.4

ABSTRACT

ABSTRACT

        A mathematical theory of secrecy systems is
developed. Three main problems are considered. (1) A
logical formulation of the problem and a study of the
mathematical structure of secrecy systems. (2) The
problem of "theoretical secrecy," i.e., can a system be
solved given unlimited time and how much material must
be intercepted to obtain a unique solution to cryptograms.
A secrecy measure called the "equivocation" is defined
and its properties developed. (3) The problem of
"practical secrecy." How can systems be made difficult
to solve, even though a solution is theoretically
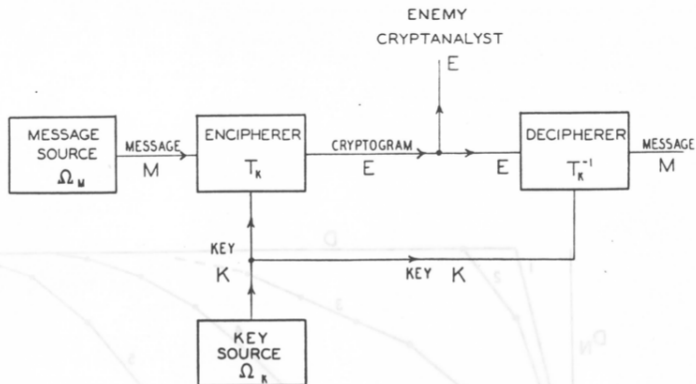possible.

Shannon: mathematical theory of communications

Figure 26: Shannon crypto diagram

The Bell System Technical Journal

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual
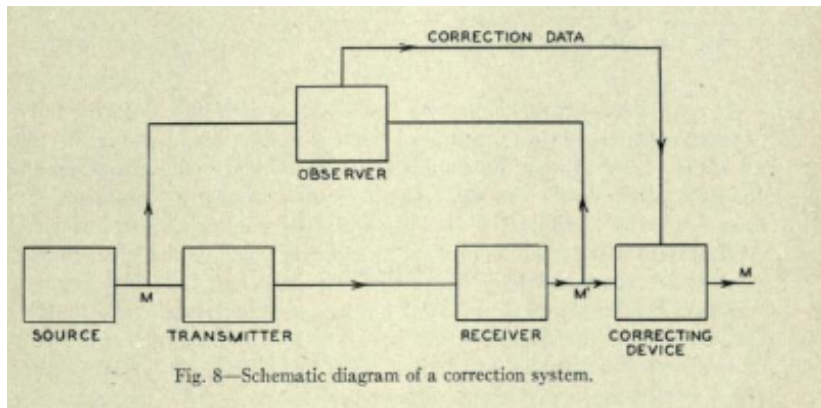
Shannon: from interception to communications

Figure 28: Shannon communications diagram

Turing on Turing

sooner or later, do so. But in the meantime, the Poles had used the duplicated transmission to identify which wheels were being used and their relative positions, using giveaways known to the British codebreakers as 'females'. Females happened when the same letter appeared in both versions of the enciphered triplet in the same place – for example, if CIL was transmitted as ABN MRN.

Figure 30: polish engineering

The Poles explained the principles behind their *bomba* machine to Dilly Knox in Poland in July 1939, a mere five weeks before the invasion. The

Figure 31: knowledge transfer
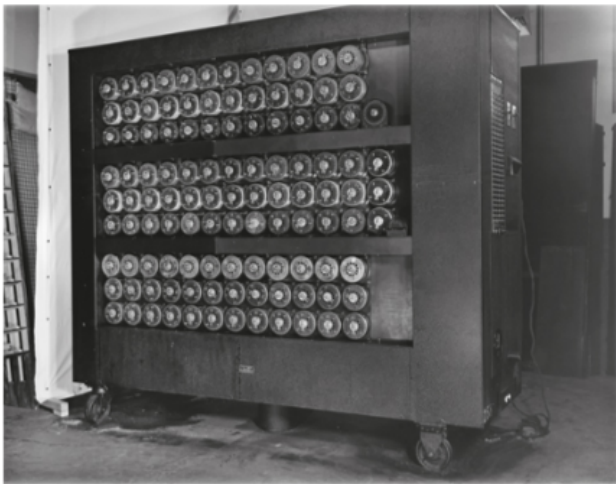
Not a computer. The Bombe, designed by Alan Turing and Gordon Welchman, found logically plausible Enigma settings which were worth testing further.

ALAN TURING'S TRIP to America was so secret that, nine years later, in writing to his friend Norman Routledge Alan said that the job he had had during the war 'certainly did not involve any travelling'. In fact, his

Figure 33: secrecy

Washington

November 28, 1942

REPORT BY DR A.M. TURING, Ph. D.

Alan was next due to visit Bell
Laboratories, the research division of
the telephone company AT&T. In many
ways this was the counterpart to the

Post Office Research Establishment
where Tommy Flowers was based, and it
was where they were building Bombes
for the US Army. Getting into Bell
Labs was difficult. For one thing the
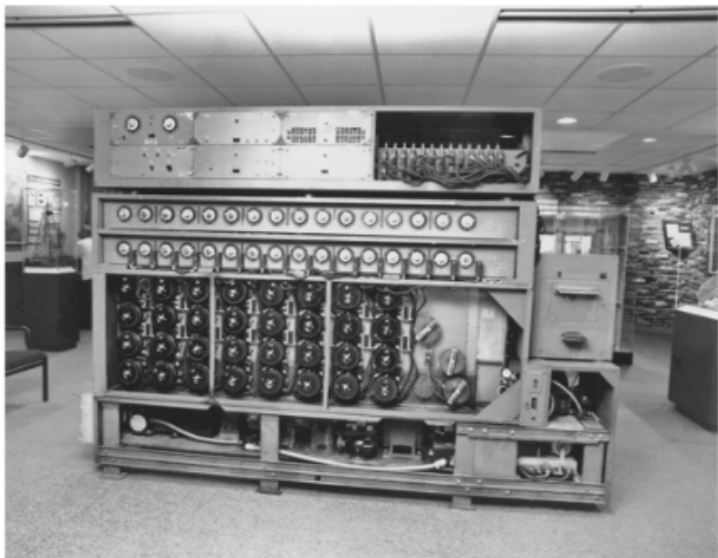
Very substantial equipment: the US
Navy's four-wheel Bombe (above), and

Lasting impact, as told by NSA

Conventional wisdom about NSA and computers has it, as a retired NSA senior officer once wrote me, "In the early days, NSA and its predecessor organizations drove the computer industry. In the 1960s, we kept pace with it. We started losing ground in the '70s, and in the '80s we struggled to keep up with the industry.

from NSA "It wasn't all magic" Colin B Burke, 1994, dec. 2002

Lasting impact

- digital computers as more than just *calculators*

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild
  - need for storage *AND* calculation

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild
  - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
    - large amounts of data accumulated in the wild
    - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations
- creation of "digital" ways to understand

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild
  - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations
- creation of "digital" ways to understand
  - belief: Turing's *bans*

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild
  - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations
- creation of "digital" ways to understand
  - belief: Turing's *bans*
  - information: Shannon's bits

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
    - large amounts of data accumulated in the wild
    - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations
- creation of "digital" ways to understand
    - belief: Turing's *bans*
    - information: Shannon's bits
- vast government patronage

Lasting impact

- digital computers as more than just *calculators*
- digital computers as *information processors*
  - large amounts of data accumulated in the wild
  - need for storage *AND* calculation
- transformation of large bureaucracies into machine organizations
- creation of "digital" ways to understand
  - belief: Turing's *bans*
  - information: Shannon's bits
- vast government patronage
  - military-industrial-academic complex

contemporary article(s) on the theme

- Mitchell + Jordan piece

power and principles

how did this capability rearrange power? who can now do what, from what, to whom?

- gender and professional roles

how did this capability rearrange power? who can now do what, from what, to whom?

- gender and professional roles
- need for engineering resources: only certain countries, companies

how did this capability rearrange power? who can now do what, from what, to whom?

- gender and professional roles
- need for engineering resources: only certain countries, companies
- secrecy

role of rights, harms, justice?

foreshadowing data for Thursday

reminder: themes for today

- hardware, labor, power

reminder: themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM...)

reminder: themes for today

- ▶ hardware, labor, power
    - ▶ the labor behind 'data' has been absent so far
    - ▶ (later we'll see labor in collection of data, census, IBM...)
    - ▶ now labor becomes visible, as computation is born

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value

reminder: themes for today

- ▶ hardware, labor, power
  - ▶ the labor behind 'data' has been absent so far
  - ▶ (later we'll see labor in collection of data, census, IBM. . .)
  - ▶ now labor becomes visible, as computation is born
  - ▶ immediately, the gendering of labor happens, segregating task + value
  - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)

reminder: themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM...)
  - now labor becomes visible, as computation is born
  - immediately, the gendering of labor happens, segregating task + value
  - "the gendered nature of technical skill [and] of labor" (-Abbate)
  - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
  - similar valuation of skills (classics, math, engineering, stats)
  - trading zones

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)
    - trading zones
    - driving problem is engineering not science

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)
    - trading zones
    - driving problem is engineering not science
- role of state and power, transfer immediately to corporations

reminder: themes for today

- hardware, labor, power
  - the labor behind 'data' has been absent so far
  - (later we'll see labor in collection of data, census, IBM...)
  - now labor becomes visible, as computation is born
  - immediately, the gendering of labor happens, segregating task + value
  - "the gendered nature of technical skill [and] of labor" (-Abbate)
  - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
  - similar valuation of skills (classics, math, engineering, stats)
  - trading zones
  - driving problem is engineering not science
- role of state and power, transfer immediately to corporations
  - UK: post office

reminder: themes for today

- ▶ hardware, labor, power
    - ▶ the labor behind 'data' has been absent so far
    - ▶ (later we'll see labor in collection of data, census, IBM. . .)
    - ▶ now labor becomes visible, as computation is born
    - ▶ immediately, the gendering of labor happens, segregating task + value
    - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
    - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
    - ▶ similar valuation of skills (classics, math, engineering, stats)
    - ▶ trading zones
    - ▶ driving problem is engineering not science
- ▶ role of state and power, transfer immediately to corporations
    - ▶ UK: post office
    - ▶ US: telecommunications, NCR, etc. . .

reminder: themes for today

- ▶ hardware, labor, power
  - ▶ the labor behind 'data' has been absent so far
  - ▶ (later we'll see labor in collection of data, census, IBM...)
  - ▶ now labor becomes visible, as computation is born
  - ▶ immediately, the gendering of labor happens, segregating task + value
  - ▶ "the gendered nature of technical skill [and] of labor" (-Abbate)
  - ▶ *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- ▶ Bayes and trading zones
  - ▶ similar valuation of skills (classics, math, engineering, stats)
  - ▶ trading zones
  - ▶ driving problem is engineering not science
- ▶ role of state and power, transfer immediately to corporations
  - ▶ UK: post office
  - ▶ US: telecommunications, NCR, etc...
  - ▶ note this is an age before the industrial-military complex

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM...)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)
    - trading zones
    - driving problem is engineering not science
- role of state and power, transfer immediately to corporations
    - UK: post office
    - US: telecommunications, NCR, etc...
    - note this is an age before the industrial-military complex
    - note this is an age before the industrial-military-academic complex

reminder: themes for today

- hardware, labor, power
    - the labor behind 'data' has been absent so far
    - (later we'll see labor in collection of data, census, IBM. . .)
    - now labor becomes visible, as computation is born
    - immediately, the gendering of labor happens, segregating task + value
    - "the gendered nature of technical skill [and] of labor" (-Abbate)
    - *continues to present* data labor increasingly 'invisible', obscuring lines and dynamics of power
- Bayes and trading zones
    - similar valuation of skills (classics, math, engineering, stats)
    - trading zones
    - driving problem is engineering not science
- role of state and power, transfer immediately to corporations
    - UK: post office
    - US: telecommunications, NCR, etc. . .
    - note this is an age before the industrial-military complex
    - note this is an age before the industrial-military-academic complex
        - 'secrecy' ties into this power

guiding questions every week:

- Scientific and mathematical development

guiding questions every week:

- ▶ Scientific and mathematical development
- ▶ Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)

guiding questions every week:

- Scientific and mathematical development
- Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)
- Driving forces: money, prestige, resources, Imperial competition... and "truth!"

guiding questions every week:

- Scientific and mathematical development
- Technologies and engineering (not so much in "part 1", more in parts 2/3 of class)
- Driving forces: money, prestige, resources, Imperial competition. . . and "truth!"
- how did new capabilities rearrange power? (who can now do what, from what, to whom?) (rights, harms, justice)

appendix

- 2020-01-21 : 1 of 14 intro to course

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI
- 2020-03-24 : 9 of 14 big data, old school (1958-1980)

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI
- 2020-03-24 : 9 of 14 big data, old school (1958-1980)
- 2020-03-31 : 10 of 14 data science, 1962-2017

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI
- 2020-03-24 : 9 of 14 big data, old school (1958-1980)
- 2020-03-31 : 10 of 14 data science, 1962-2017
- 2020-04-07 : 11 of 14 AI2.0

appendix

- ▶ 2020-01-21 : 1 of 14 intro to course
- ▶ 2020-01-28 : 2 of 14 setting the stakes
- ▶ 2020-02-04 : 3 of 14 risk and social physics
- ▶ 2020-02-11 : 4 of 14 statecraft and quantitative racism
- ▶ 2020-02-18 : 5 of 14 intelligence, causality, and policy
- ▶ 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- ▶ 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- ▶ 2020-03-10 : 8 of 14 birth and death of AI
- ▶ 2020-03-24 : 9 of 14 big data, old school (1958-1980)
- ▶ 2020-03-31 : 10 of 14 data science, 1962-2017
- ▶ 2020-04-07 : 11 of 14 AI2.0
- ▶ 2020-04-14 : 12 of 14 ethics

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI
- 2020-03-24 : 9 of 14 big data, old school (1958-1980)
- 2020-03-31 : 10 of 14 data science, 1962-2017
- 2020-04-07 : 11 of 14 AI2.0
- 2020-04-14 : 12 of 14 ethics
- 2020-04-21 : 13 of 14 present problems: attention economy+VC=dumpsterfire

appendix

- 2020-01-21 : 1 of 14 intro to course
- 2020-01-28 : 2 of 14 setting the stakes
- 2020-02-04 : 3 of 14 risk and social physics
- 2020-02-11 : 4 of 14 statecraft and quantitative racism
- 2020-02-18 : 5 of 14 intelligence, causality, and policy
- 2020-02-25 : 6 of 14 data gets real: mathematical baptism
- 2020-03-03 : 7 of 14 WWII, dawn of digital computation
- 2020-03-10 : 8 of 14 birth and death of AI
- 2020-03-24 : 9 of 14 big data, old school (1958-1980)
- 2020-03-31 : 10 of 14 data science, 1962-2017
- 2020-04-07 : 11 of 14 AI2.0
- 2020-04-14 : 12 of 14 ethics
- 2020-04-21 : 13 of 14 present problems: attention economy+VC=dumpsterfire
- 2020-04-28 : 14 of 14 future solutions