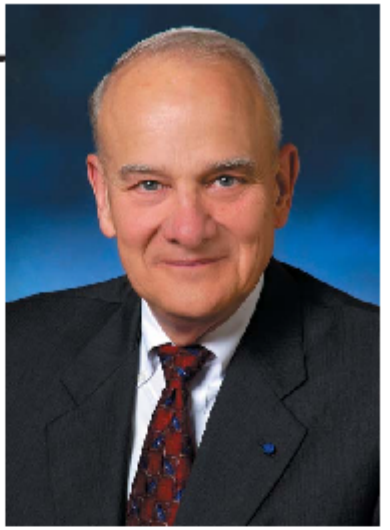
Friday Office Hours

- If it doesn't rain (and no one else is there), I'll be in Darden Courtyard from 2:00 to, say, 4:30
- Answering CS 415 questions and **fencing**
- Free: we provide all the gear, lessons, etc.
  - No experience needed
- Have some PA frustrations?
- Take them out on me!

CS 415 Last Year ->

Recall Bill Wulf



April 30th 3 - 5 pm
Harrison Library Auditorium

It could be the biggest scandal since the founding of the CS Department 40 years ago!

Bill Wulf's dissertation is unsigned! Did we really let our first graduate go off and build one of the best CS departments in the country, start a company, hold an official position in the National Scicence Foundation and lead the premier body of engineers for 11 years without officially holding his doctorate?

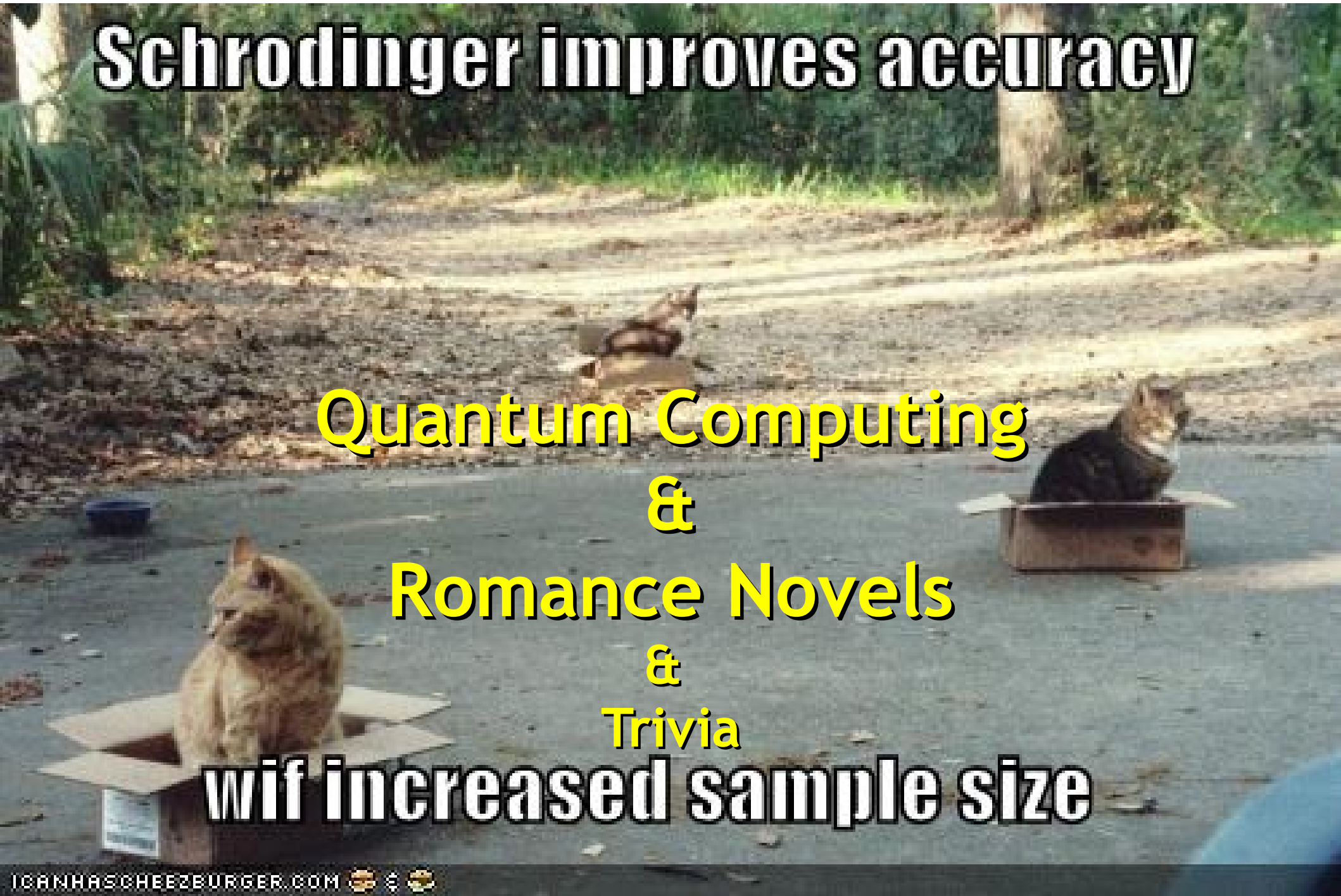
Find out on April 30th whether Bill really deserves that Doctor of Science UVA SEAS gave him 40 years ago this semester. Witness members of his original defense committee grill him on the particulars of his work.

Ask some questions yourself!

Hear Bill try to explain the relevance of his work to first year undergraduate majors. Enjoy the refreshments and camaradarie as we

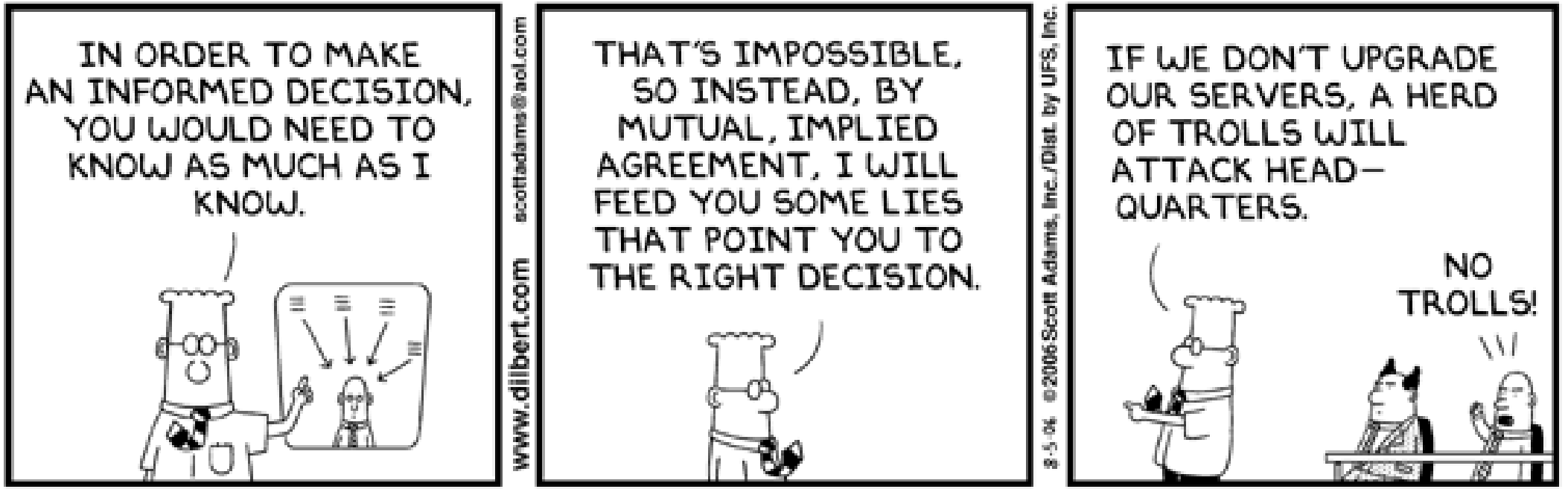
Recall Bill Wulf

From 20 years of National Service
For 40 years of great contributions
As a potential imposter in need of proving he earned his degree!


Schrodinger improves accuracy
Quantum Computing
&
Romance Novels
&
Trivia
wif increased sample size
ICANHASCHEEZBURGER.COM

Lies

- This lecture will gloss over most details.



- You actually know more than I know, I just don't have time to get into it.
- Next semester: **Math 540 Intro To Quantum Computing**

One-Slide Summary

- A **quantum computer** manipulates **quantum bits**; such qubits can represent a **superposition** of possible states.
- Quantum computers are **probabilistic**. **Grover's Algorithm** (for linear search in sub-linear time) and **Shor's Algorithm** (for factoring integers in polylog time) are common quantum algorithms.
- When you use a quantum computer to “try everything in parallel” you get back a **random answer**.

Theory and Practice

- Quantum Computers do not yet exist
- But we can still talk about them in theory
- Serious experimental work remains to be done!

Quantum Computers

- A **quantum computer** uses quantum effects, such as superposition or entanglement, to perform operations on data.
  - Quantum Computers ***do not exist*** (yet).
- Classical Bit: 0 *or* 1
- Quantum Bit or **Qubit**: 0 *or* 1 *or* quantum superposition of 0 and 1
  - 3 Bits = exactly one state (= one number 1-8)
  - 3 Qubits = up to 8 states simultaneously!

Quantum Digital Logic Design

- Qubits are manipulated by **quantum gates**
  - Just as AND, OR and NOT gates manipulate bits
  - There is a notion of a complete set of gates
    - AND, OR and NOT for classical
    - Hadamard, Phase Rotation and Controlled Not for Q
- Quantum gates are unitary matrices
  - Each quantum gate is **reversible**
  - This is not obvious
- One builds quantum circuits out of quantum gates

Quantum Storage

- A **quantum register** (qregister) holds qubits
  - A qregister is described by a wavefunction where the coefficients are *complex* numbers whose amplitudes squared are the probabilities to measure the qubits in each state ...
  - Complex numbers means the phases can constructively and destructively **interfere**
- Recording or simulating the state of a qregister requires an **exponential** number of classical complex numbers
  - 3-qubit qregister == 8 complex numbers
  - 300-qubit qregister == 10^{90} > |universe|

Quantum Computation

- Initialize n-qubit qregister to starting values
- Each step: n qubits go through quantum gates
  - (i.e., are multiplied by unitary matrices)
- Read qregister via **quantum measurement**
  - Yields a ***random*** n-bit string
  - And ***destroys*** the stored state as well
- This sounds **bad**
  - But: run whole program many times (i.e., sampling)
  - Probability distribution of output string is skewed in favor of the right answer

Probabilistic

- Quantum Computers are **probabilistic**
  - Repeated runs of qcomputer plus majority polling of the outputs yields the right answer with high probability
- They are *not* deterministic
  - Officially, they can get the "wrong" answer, just like that probabilistic program analysis from last week
    - Exceptions: Deutsch-Jozsa, etc.
  - In practice this is not a problem: rerun until prob of error is less than prob of earth exploding, etc.

Database Search Problem

- **Database Search Problem:**
  - To Solve: guess random answers and check them
  - There are ***n*** possible answers
  - Each guess takes the same time to check
- Example Uses:
  - Searching for an entry in an unsorted array
  - Guessing your friend's password
  - Attacking symmetric ciphers (AES, 3DES)
- Classical Running Time: **O(n)** linear search
  - Average Case: (n+1)/2 guesses to find answer

Enter Lov Grover in 1996

- **Grover's Algorithm**
  - Quantum algorithm for solving the database search problem (i.e., for doing linear search)
  - Takes **$O(\sqrt{N})$** time (yes, sqrt(N) time!)
  - Uses **$O(\log_2 N)$** qubits of storage
  - Probability of measuring wrong answer: **$O(1/N)$**
  - Algorithm is optimal
- I will not explain Grover's Algorithm.
- Instead, we will cover Shor's Algorithm.

Let's Break RSA

- Break RSA == find factors of large integer ***N***
- No known polynomial classical algorithms
  - General Number Field Sieve: ~ $O(2^b)$
  - ***b*** is number of bits in ***N*** (e.g., *b*=512)
- Could use Grover
  - Linear search for factors in $\mathbf{O(\sqrt{2^b}) = O(2^{b/2})}$ time
  - Still too slow!
- New Proposed Quantum Approach
  - Try all factors in parallel, pick the right one!
  - Does this work?

Itty Bitty Living Space

- Despite popular rumors, quantum computers *cannot easily* "try everything in parallel"
- Sure, you can try everything in parallel
- But when you measure the outcome, you get something **random**!
- In this case, you'd get a random (non-)divisor
- Which is not what we want!
  - Using the power of quantum computing to look for a needle in a haystack is not efficient!
- So we must exploit the structure of the problem

Needles In Haystacks

- Quantum computing can give you a random answer back
  - So the trick is to make sure that even a random answer will help you
  - By making sure that all answers have some important property that contributes to what you really want to know
- Look: if you think about quantum computing in terms of “parallel universes” (and whether you do or don’t is up to you), there’s no feasible way to detect a single universe that’s different from all the rest. Such a lone voice in the wilderness would be drowned out by the vast number of suburb-dwelling, Dockers-wearing conformist universes. What one can hope to detect, however, is a joint property of all the parallel universes together — a property that can only be revealed by a computation to which all the universes contribute. [Scott Aaronson]

Digression: Periodic Sequences

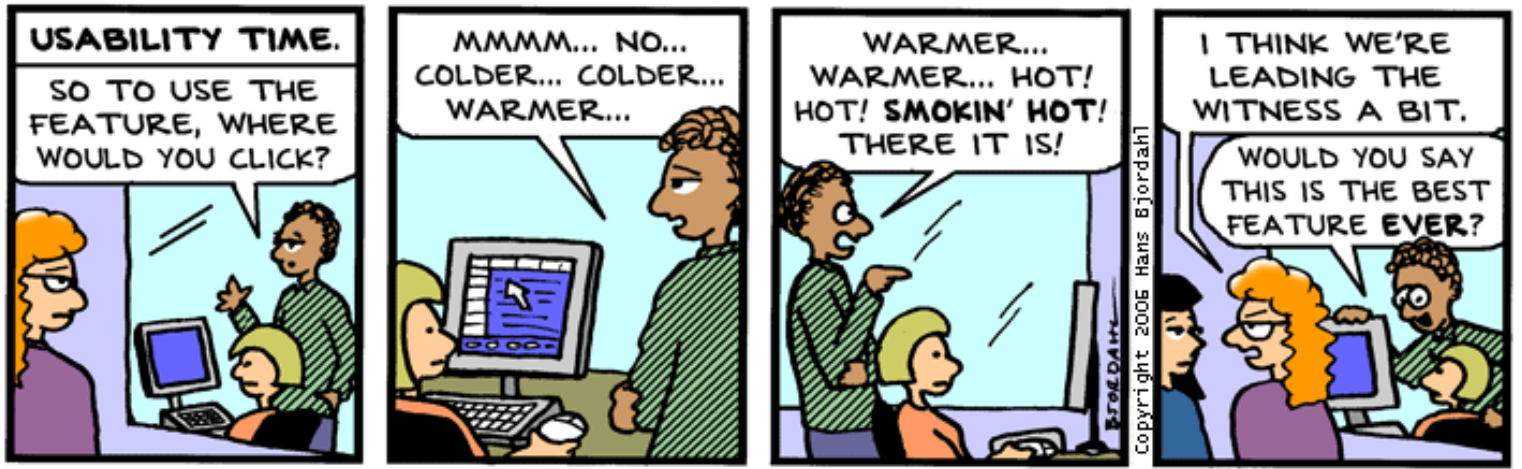
- Powers of Two: 2, 4, 8, 16, 32, 64, 128, 256, ...
  - Not a periodic sequence.
- Powers of Two Mod 15: 2, 4, 8, 1, 2, 4, 8, 1, ...
  - **Period** is 4
- Powers of Two Mod 21: 2, 4, 8, 16, 11, 1, 2, 4, ...
  - **Period** is 6
- Let N be the product of two primes p * q
  - Series: x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...
  - Has period that evenly divides (p-1)(q-1) [Euler ~1760]

Quantum World Series

- Thus ***if*** we can find the period of
  - x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...
- ***Then*** we learn something about the prime factors of N!
  - In particular, we learn a divisor of (p-1)(q-1)
  - Not as good as learning p and q themselves ...
  - But if we run it a few times and get several random divisors of (p-1)(q-1)
  - Then we can put them together to get (p-1)(q-1)
  - And then use some math tricks recover p and q

Reduction To Nowhere?

- The sequence
  - $x \bmod N$, $x^2 \bmod N$, $x^3 \bmod N$, $x^4 \bmod N$, ...
- Will *eventually* start repeating, but the number of steps before a repeat could be O(N)
  - And N was already huge!
  - Which is why this is not a good *classical* algorithm



Q: Theatre (011 / 842)

- Complete the song verse from Rodgers and Hammerstein's 1949 musical **South Pacific** that begins *"I'm gonna wash that ..."*.

Q: TV (070 / 842)

- This 1993-1998 Emmy Award-winning CBS series featured Jane Seymour as Dr. Mike. It was originally targeted at the 18-to-40 demographic but ended up viewed predominantly by women aged 40 or older.

Q: Music (123 / 842)

- Name the song: *"He was a famous trumpet man from old Chicago way. He had a boogie style that no one else could play. He was the top man at his craft, but then his number came up and he was gone with the draft. He's in the army now a-blowin' reveille."*

Q: Music (205 / 842)

- This 19th century Russian composer created the piano suite **Pictures At An Exhibition**. It includes a "Tuileries" theme depicting children playing in a garden near the Louvre.

Q: Movies (267 / 842)

- Name the movie described below, its heroine and its star. This 1979 Ridley Scott movie began the first major American film series with a female action hero.

Q: Movies (322 / 842)

- In this 1984 movie one of the villains is the Stay Puft Marshmallow Man.

Q: Movies (374 / 842)

- In this 1989 family comedy the children of Rick Moranis spend most of the day playing with bugs in the yard.

Captain Quantum

- So let's make a superposition over all of the numbers in our sequence:
  - $x \bmod N$, $x^2 \bmod N$, $x^3 \bmod N$, $x^4 \bmod N$, ...
- Then perform some quantum operation over all of them to reveal the period
- We're no longer looking for needles in haystacks
- The period is a **global property** of all of the numbers in the sequence taken together

The Key

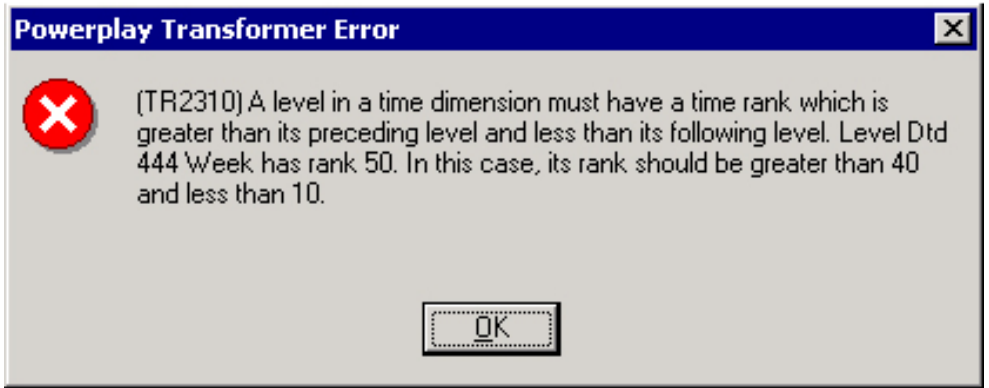
- The key to quantum algorithms is to make a bunch of parallel worlds that all have something (part of the right answer) **in common**.

Shor's Algorithm

- Let's assume we've made our superposition
  - $x \bmod N$, $x^2 \bmod N$, $x^3 \bmod N$, $x^4 \bmod N$, ...
- So, given a superposition of elements in a periodic sequence, how do we extract the period?
- We use the **Quantum Fourier Transform**
  - The heart of **Shor's Algorithm** (1994)
- Reasoning by analogy time!

Sleepless In Seattle

- Let's say your body functions on a 26-hour cycle
- Then if you had no appointments and good window blinds, you might wake up at 8am one day, 10am the next day, noon the next day, etc.
- If you were on a 27-hour cycle, it would be 8am, 11am, 2am, etc.
- So, if I see you waking up at 8am, can I tell what kind of cycle you're on?

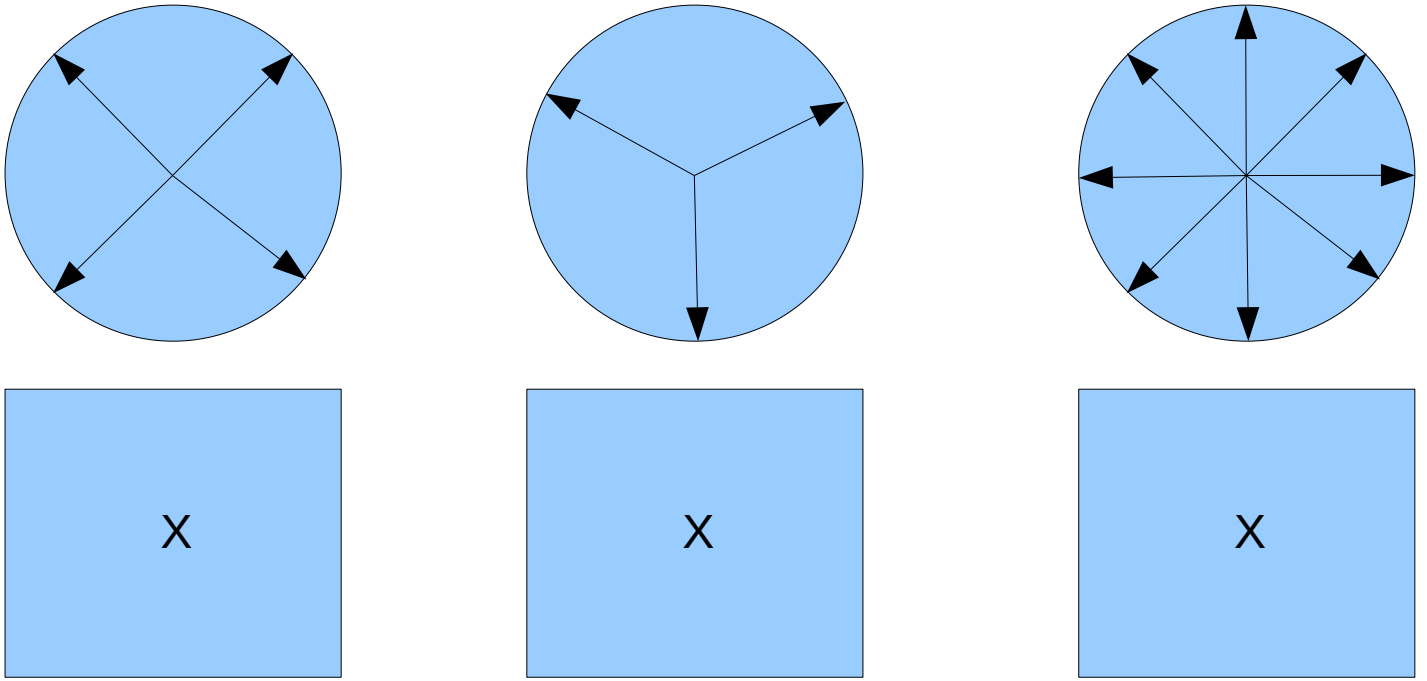


Groundhog Day

- Let's imagine that your bedroom has many clocks in it
  - Each clock has an hour hand (no minute hand)
  - One clock has 26 hours per day
  - One clock has 27 hours per day
  - One clock has 3 hours per day, etc.
  - Each hour is still 60 minutes on all clocks
- Each clock has its own posterboard with a thumbtack in it – mounted right below the clock
  - When you wake up, you move each thumbtack in the direction of its clock's hour hand

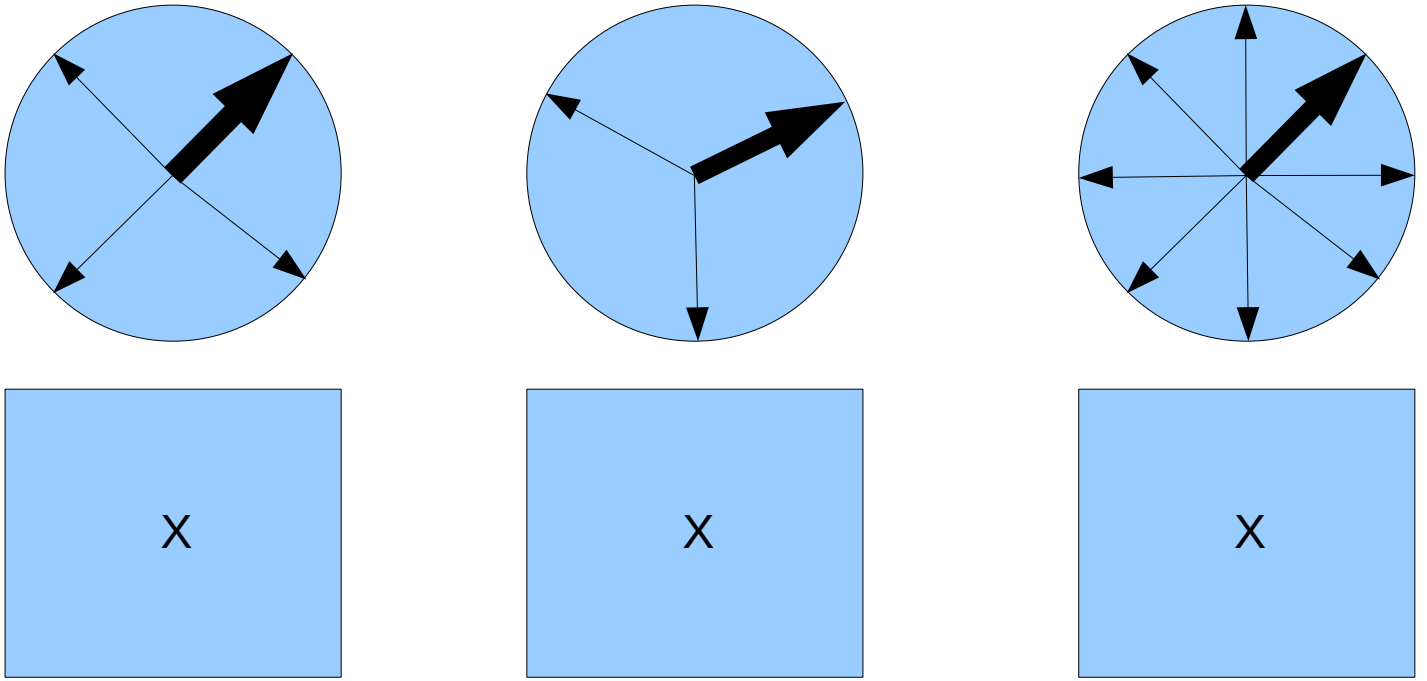
Bedroom Of Doom!

- Three of your clocks: 4-hour, 3-hour, 8-hour:



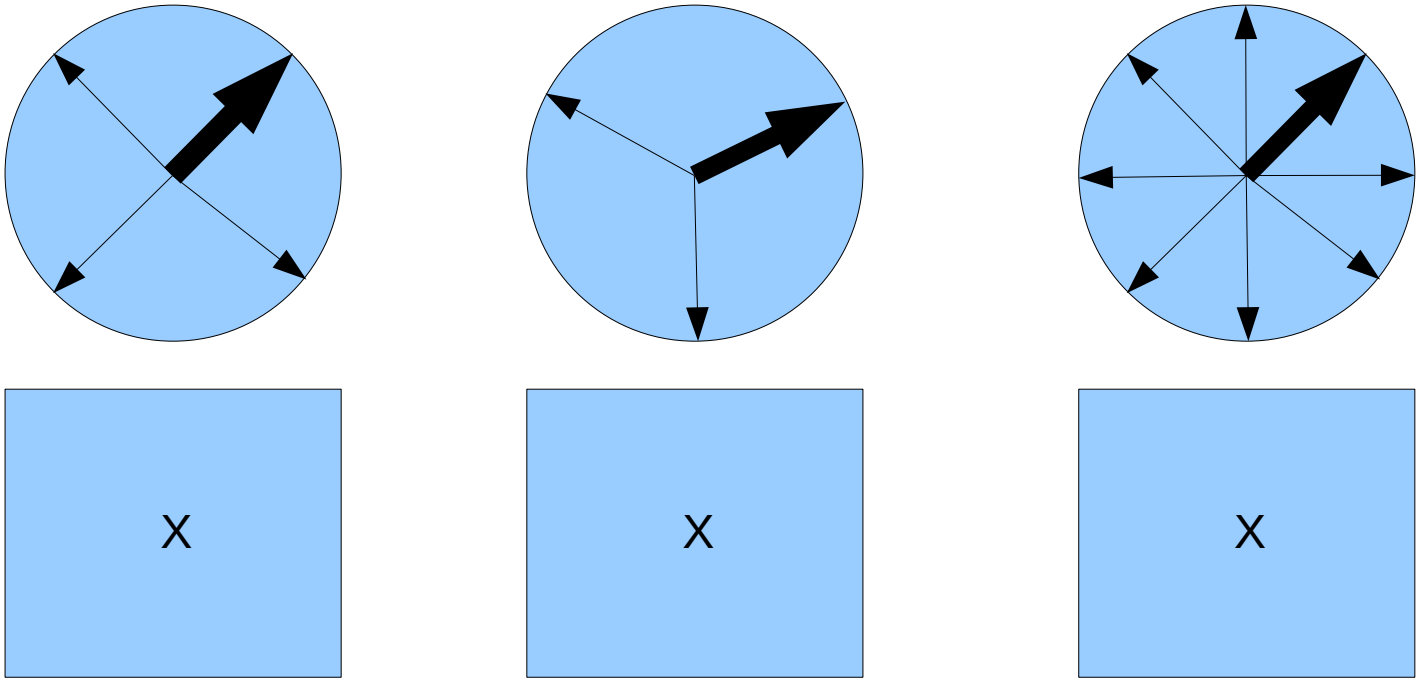
Bedroom Of Doom! (1pm)

- Let's say the current time is 1pm on all clocks.



Bedroom Of Doom! (1pm)

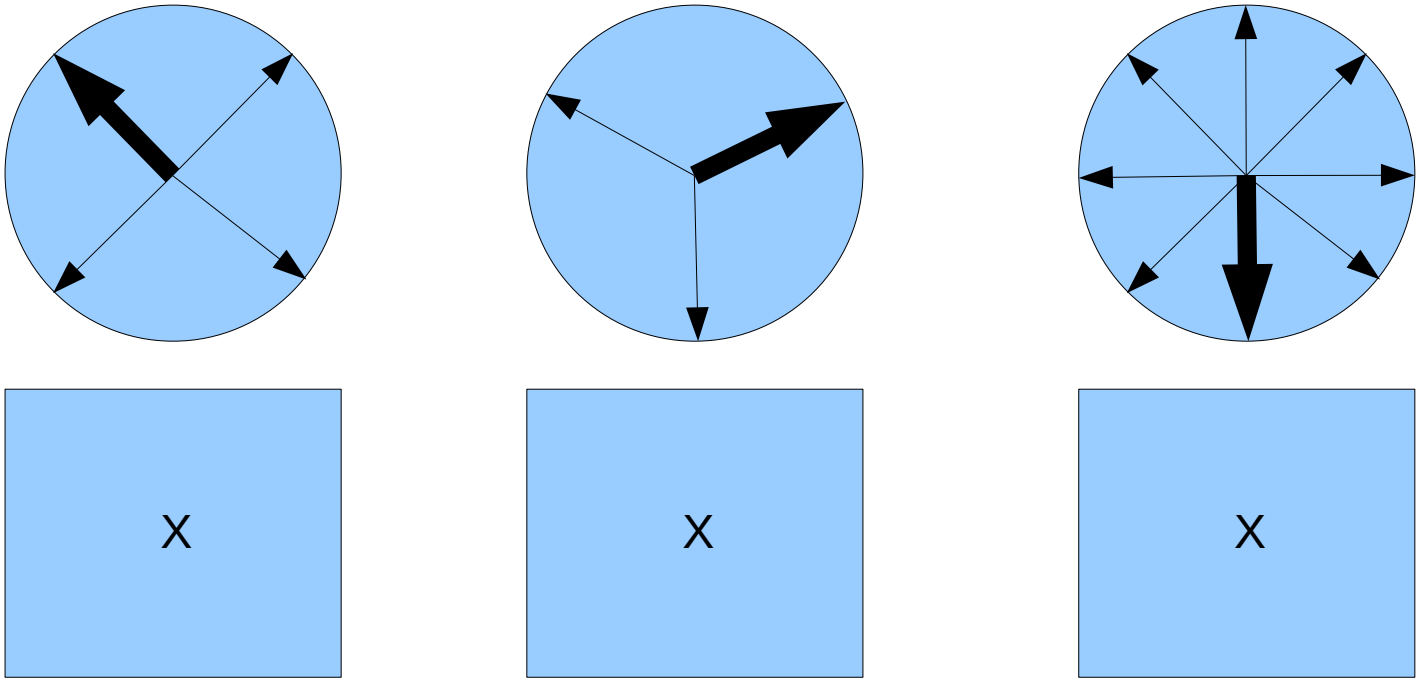
- Let's say you're on a 3-hour day, so you wake up every three hours.



- So when next you wake up, it'll be three hours later ...

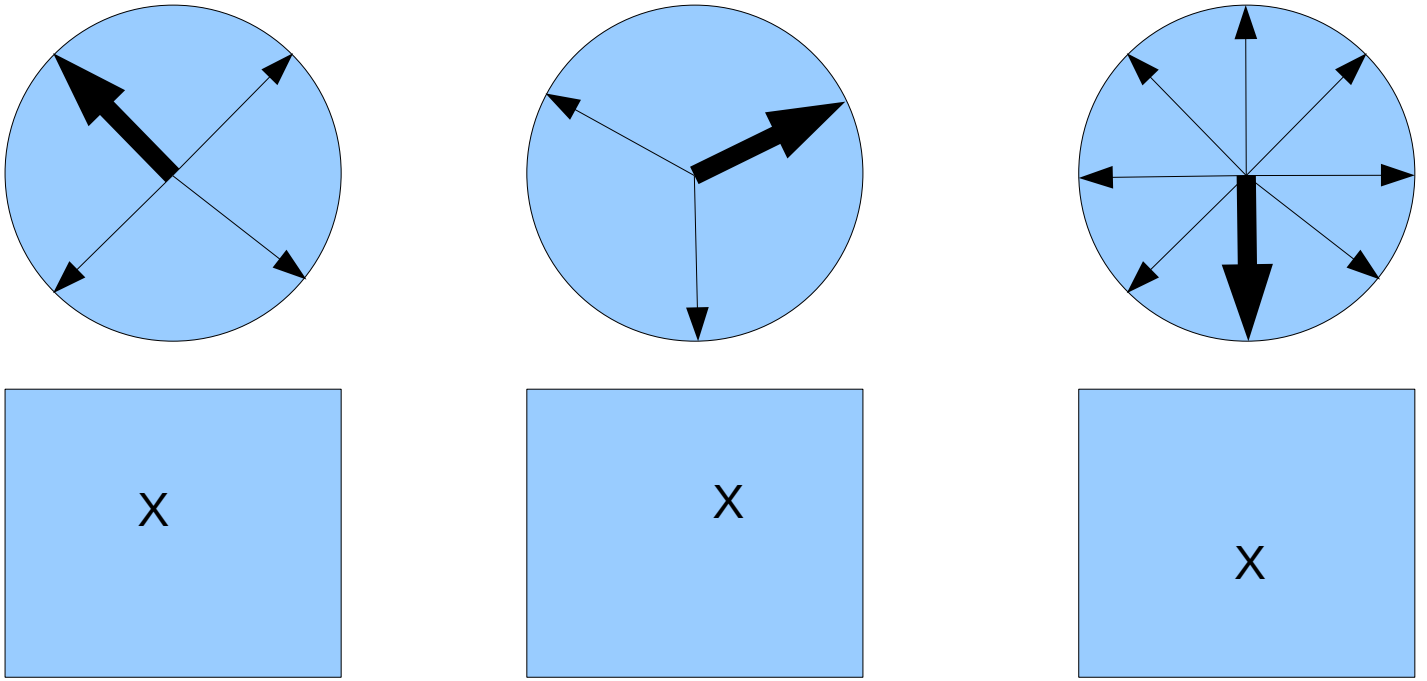
Bedroom Of Doom! (4pm)

- So you adjust the clocks



Bedroom Of Doom! (4pm)

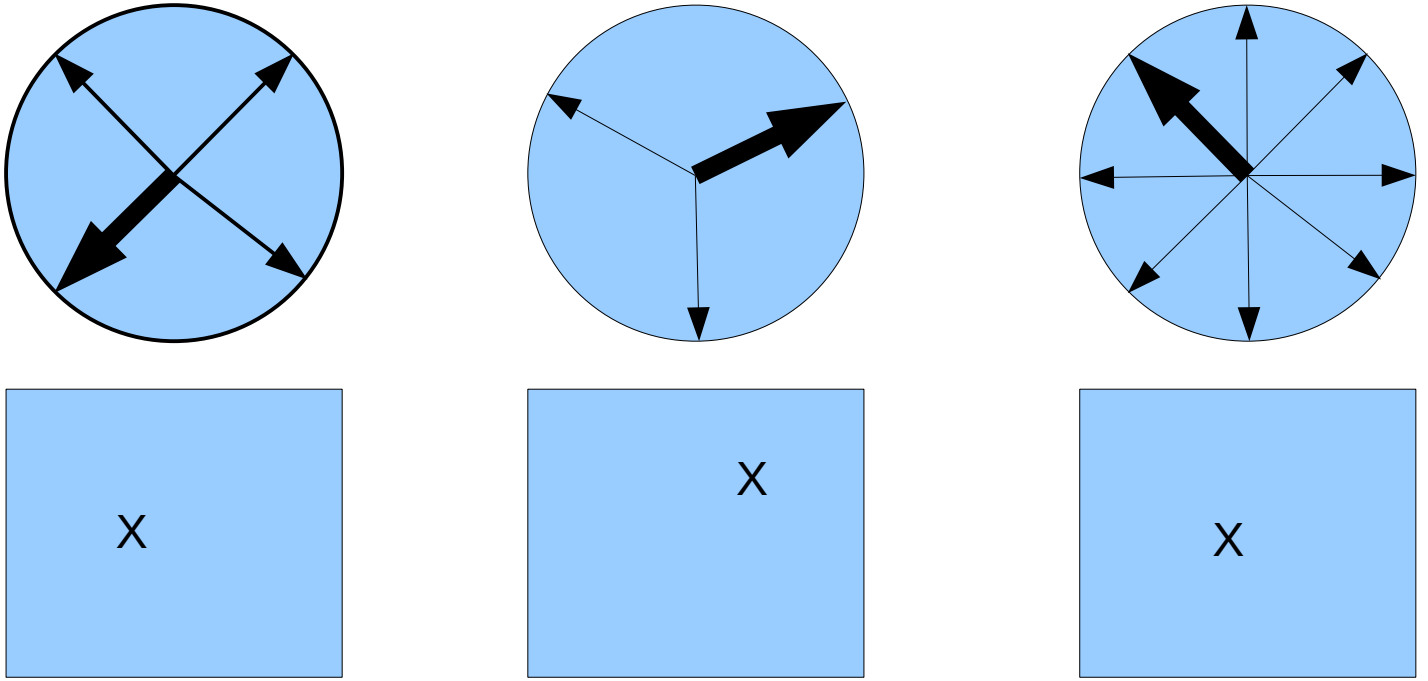
- So you adjust the clocks



- And move the thumbtacks ...

Bedroom Of Doom! (7pm)

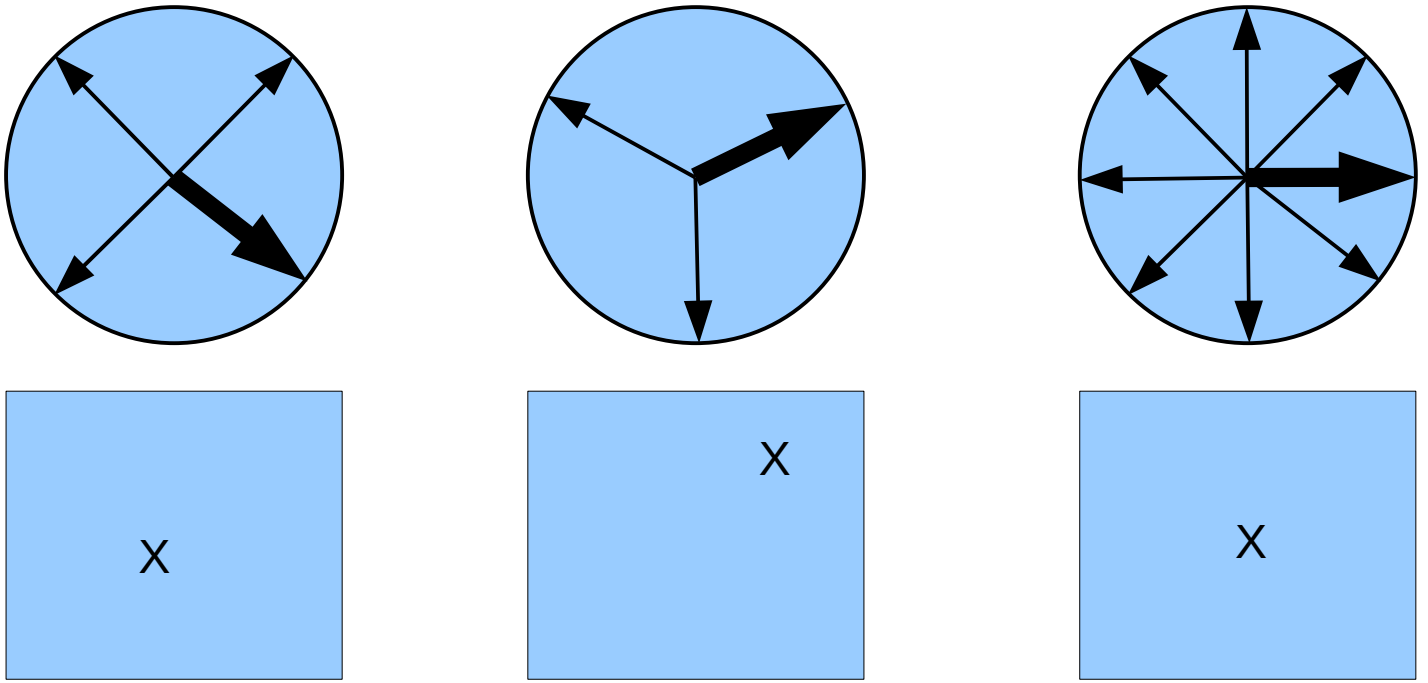
- Wakey Wakey! So you adjust the clocks



- And move the thumbtacks ...

Bedroom Of Doom! (10pm)

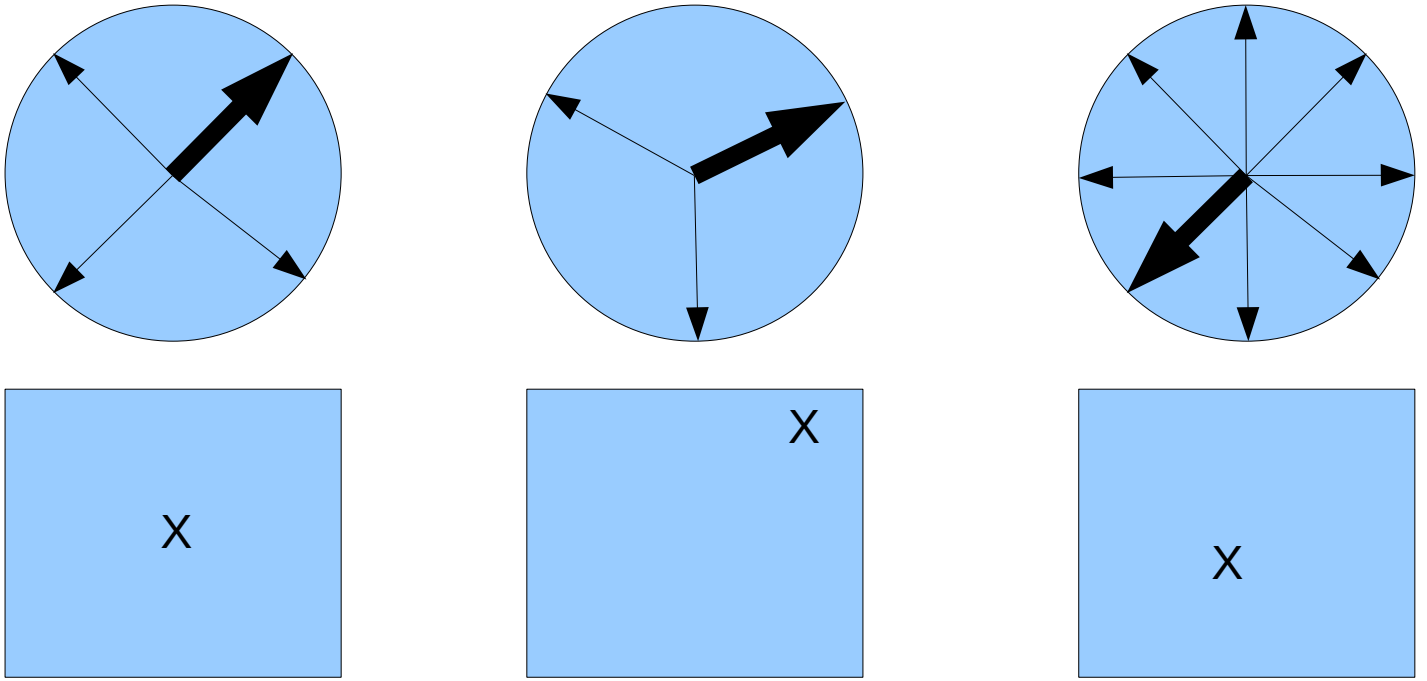
- Wakey Wakey! So you adjust the clocks



- And move the thumbtacks ...

Bedroom Of Doom! (1am)

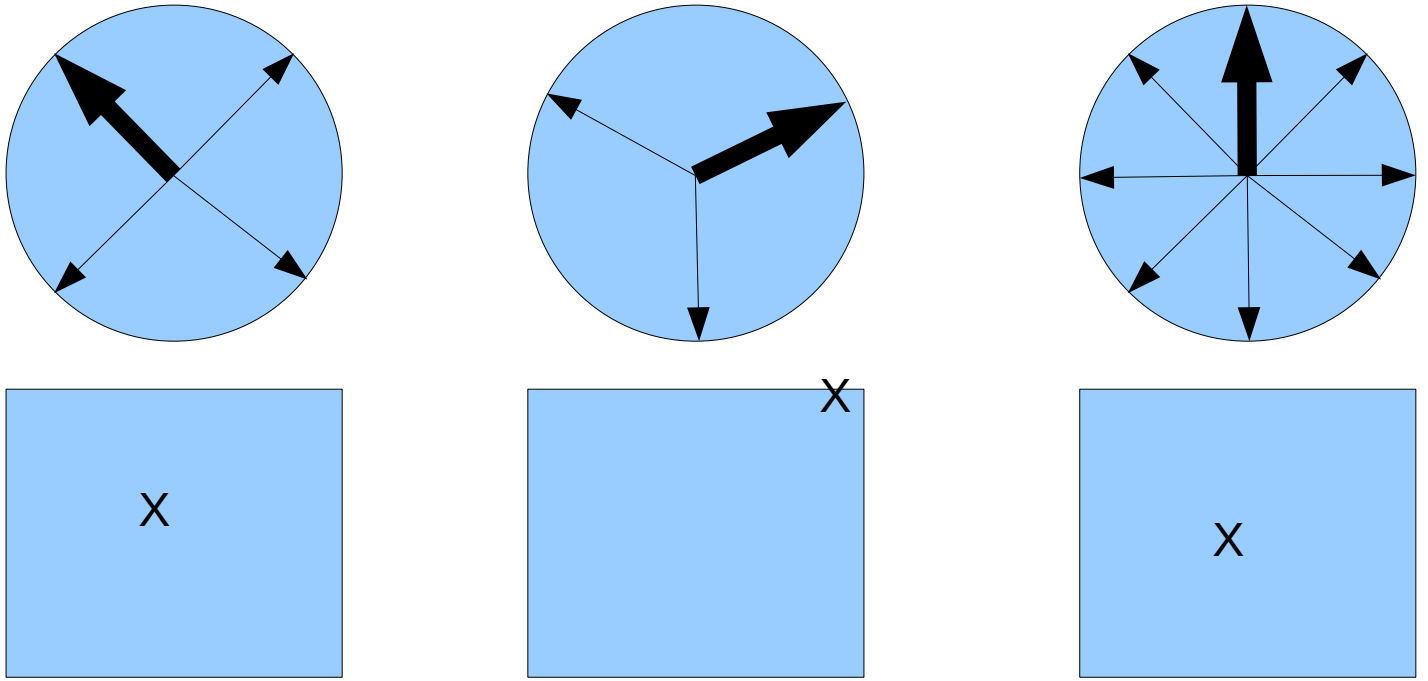
- Sigh! So you adjust the clocks



- And move the thumbtacks ...

Bedroom Of Doom! (4am)

- Sigh! So you adjust the clocks



- *How can you tell which clock matches your period?*

Periodic Motion

It's Just A Jump To The Left

- If you're on a 3-hour day, the 4-hour clock's thumbtack drifts around a little, but every few days it returns to the center
  - All of the movements cancel each other out!
- On the other hand, from the perspective of the 3-hour clock you've been waking up at the same time each “morning”
  - **So you keep moving that thumbtack in the same direction!**
- So just find which thumbtack is farthest from the center and you've found the period.

QFT, QED.

- The **Quantum Fourier Transform** is a linear (unitary) transformation that maps a vector of complex numbers to another vector of complex numbers
- Input vector has nonzero entries every time I wake up, zero entries everywhere else
- Output vector records thumbtack positions
- In the end: it's a linear transform mapping quantum state encoding a periodic sequence to a quantum state encoding the *period* of the sequence!

Interference

- In quantum-land, probabilities are always non-negative but **amplitudes** may be negative, positive or even complex.
- Thus amplitudes corresponding to different ways of getting a particular answer can **intefere destructively** and cancel each other out
- In Shor, all periods from all observations (i.e., all alternate universes) other than the true one cancel each other out. Only for the true period do contributions from all observations (i.e., all universes) point in the same direction.

Shor's Algorithm

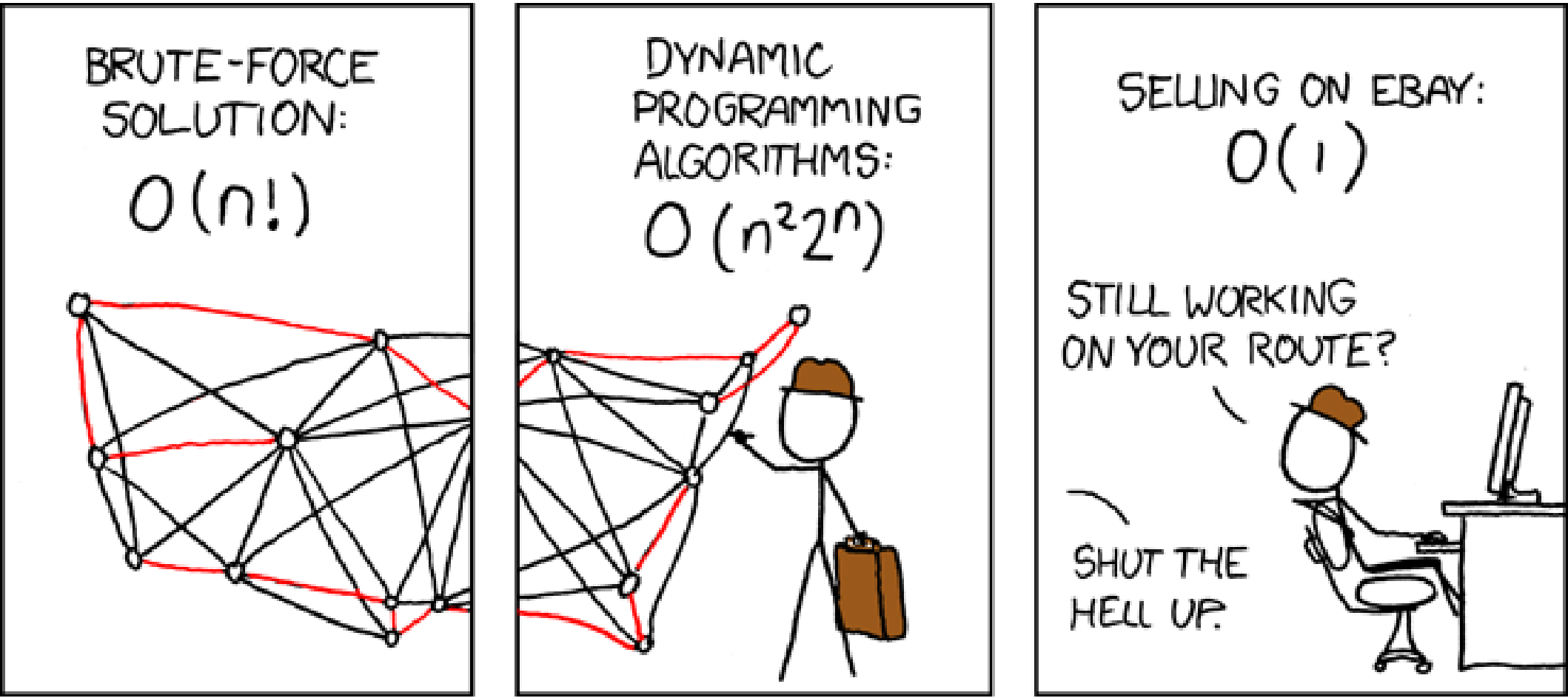
- On a quantum computer, **Shor's Algorithm** takes $O((\log N)^3)$ time to factor the integer N
  - Recall: best classical time ~$O(2^{\log N})$
- In 2001, a team at IBM implemented Shor's algorithm and factored 15 using 7 qubits
  - *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*
  - "We use seven spin-1/2 nuclei in a molecule as quantum bits, which can be manipulated with room temperature liquid-state nuclear magnetic resonance techniques."

Did We Win?

- A normal Turing machine can simulate a quantum computer (slowly ...)
  - So we do not gain any expressive power
  - Quantum computers do not solve the halting problem
- But quantum computers sure seem faster!
- The class of problems that can be solved efficiently by quantum computers is called **BQP** (bounded error, quantum, polynomial time).

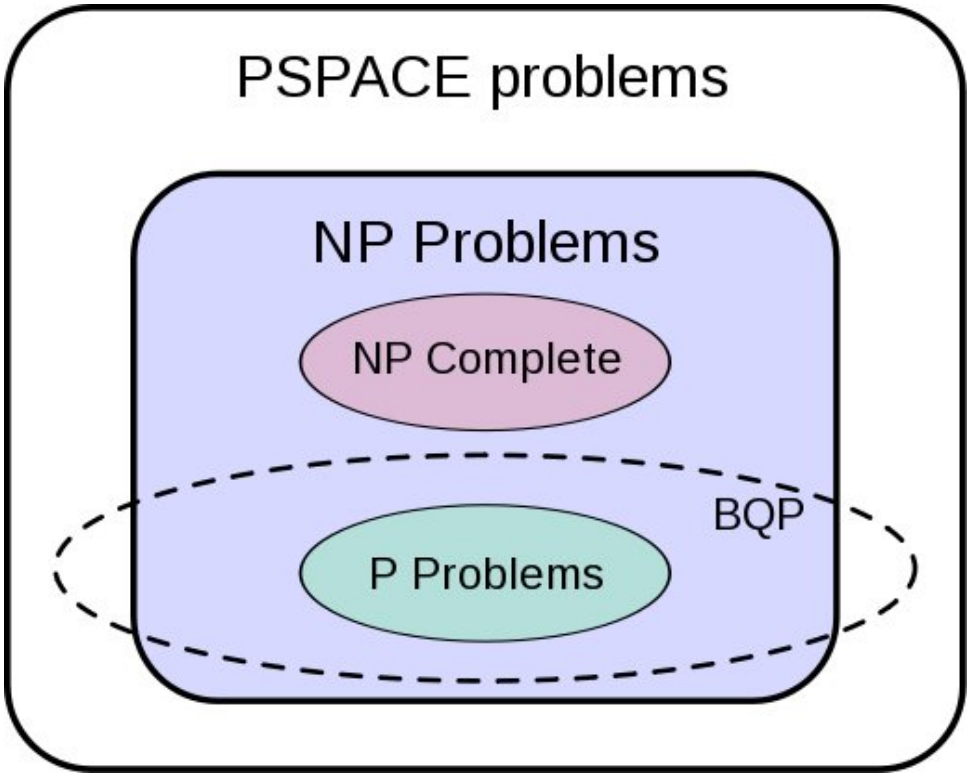
P = NP ?

- **So**: “quantum computers can solve NP-complete problems in polynomial time” ?



P = NP ?

- **Misconception**: “quantum computers can solve NP-complete problems in polynomial time”
- BQP is *suspected* to be a superset of P and disjoint from NP (this is *unknown*)



What Is Quantum Good For?

- BQP contains Integer Factorization
  - Believed to be in NP but not in P
- BQP contains Discrete Log
  - Believed to be in NP but not in P
- BQP contains Quantum Database Search
  - Can give an N^2 speedup on any NP-complete problem (by searching through all the answers), but that's still exponential time
- And that's currently about it.

Q: Movie Music (437 / 842)

- This most common word in the 1991 Disney song **Belle** remains the same in the French localization of the movie.

Q: General (481 / 842)

- In 1983 this man challenged the major findings of Margaret Mead, a famous cultural anthropologist, five years after she died. He based his highly questionable critique on four years of field experience and recent interviews with survivors of Mead's original study.

Q: Games (543 / 842)

- His genre-spawning 1993 game, "affectionately" referred to as "crack for gamers", was later inducted into the **GAMES Magazine** and **Origins** Halls of Fame. Name this game designer, who also holds a doctorate in mathematics.

Q: Events (607 / 842)

- This Palestinian "uprising", sometimes called "the war of the stones", began on December 8, 1987.

Q: Cartoons (663 / 842)

- Give all four Renaissance artist names chosen by Splinter the Rat for his four mutant ninja disciples in the 1984 comic book and 1987 cartoon.

Q: Books (731 / 842)

- This 1958 ursine children's book character was created by Michael Bond. He likes marmalade and is known for the railway station where he was found.

Q: Advertising (833 / 842)

- This company's hosiery first came in plastic egg containers in 1970.

Q: Advertising (840 / 842)

- In their 1987 ad campaign The Partnership For A Drug-Free America used the phrase *"This is your brain. This is your brain on drugs. Any questions?"* What was used to symbolize *"your brain"* ? The ads were directed by Joe Pytka.

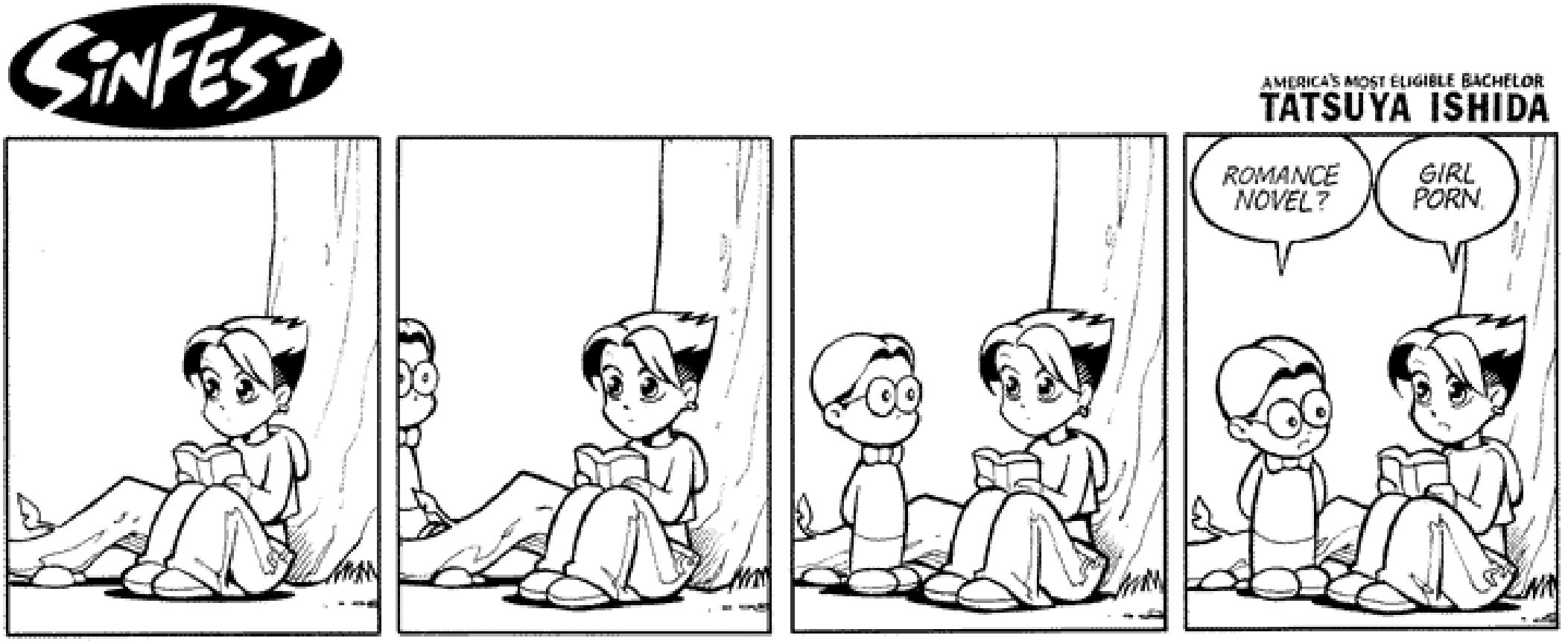
Harlequin Segue!

- "Don't come back until you have him", the Tick-Tock Man said quietly, sincerely, extremely dangerously.
- They used dogs. They used probes. They used cardio plate crossoffs. They used teepers. They used bribery. They used stick tites. They used intimidation. They used torment. They used torture. They used finks. They used cops. They used search and seizure. They used fallaron. They used betterment incentives. They used finger prints. They used the bertillion system. They used cunning. They used guile. They used treachery. They used Raoul-Mitgong but he wasn't much help. They used applied physics. They used techniques of criminology. And what the hell, they caught him.

  - Harlan Ellison: Repent, Harlequin, said the Tick-Tock Man

Dispelling Romance Novel Myths

- Tell me something about romance novels ...



Why Should We Care?

- In North America, romance novels comprise 55% of all paperbacks sold
  - Most popular genre in modern literature
  - And 39% of all fiction sold
  - Also Europe & Australia, over 90 languages, etc.
- In 2004, romantic fiction generated $1.2 billion in sales (2285 separate novels that year)
  - 64 million people claimed to read at least one in 2004 (up 21% from 2001)
  - 22% male, 50-50 married/single, 42% BA/BS
  - 28/190 world countries have GDP < $1.2 billion

What Are We Talking About?

- According to the Romance Writers of America, the main plot of a **romance novel** must revolve around the two people as they develop romantic love for each other and work to build a relationship together. Furthermore, a romance novel must have an "emotionally satisfying and optimistic ending."
- Nora Roberts claims "The books are about the celebration of falling in love and emotion and commitment, and all of those things we really want."

Freedom?

- Modulo societal taboos, almost anything can appear in a romance novel.
  - Castles, domestic violence, science fiction, disabilities, children, religion, date rape, medicine, suspense, exotic locales, chaste kisses, etc.
- So let's do a brief history and taxonomy of romance novels and occasionally use them as a lens for studying society

Ancient History

- 1740: Pamela, or Virtue Rewarded by Samuel Richardson
  - First popular novel based on heroine's perspective
- 1813: Pride and Prejudice by Jane Austen
  - Often critically considered “the best romance novel ever written”
  - Reinforces stereotype that women must marry?
- 1847: Jane Eyre by Charlotte Bronte
  - Orphaned heroine, gothic elements, Elizabethan drama, “demonstrated the flexibility of the romance novel form”

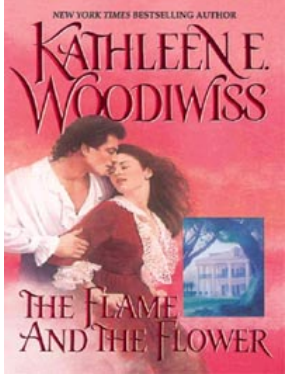
History

- 1919: The Sheik by E.M. Hull
  - Popular, movie with Valentino, hero kidnaps heroine and wins her affection through “forceful action”
    - One of the first to introduce the rape fantasy [Regis 2003]. Publishers believed that readers would only accept premarital sex in the context of rape. In this novel and those that followed, the rape was depicted as more of a fantasy; the heroine is rarely if ever shown experiencing terror, stress, or trauma as a result.
- 1921+: Many by Georgette Heyer
  - Set during English Regency Period (1811-1820)
  - Used setting as a plot device: characters would have modern day sensibilities (e.g., marrying for love) and would be marked as eccentric

Pre-Modern Era

- 1930+: Mills and Boon hardback romances
  - UK Company, sold in weekly two-penny libraries
- 1957: Harlequin sells M&B books in America
  - Had a “decency code”
    - cf. Hays Production Code in US Cinema, 1934-1968: replaced by MPAA ratings
    - Intimacy limited to chaste kisses between protagonists
- 1971: Harlequin purchases Mills & Boon
  - Chose to sell books “where the women are”: supermarkets, drug stores, etc.

The Modern Era



- 1972: The Flame and the Flower by Kathleen Woodiwiss (Avon publishers)
  - First romance novel “to [follow] the principles into the bedroom”; first to be published directly in paperback; was distributed in drug stores; went on to sell 2.35 million copies
- By 1975 Avon's 4 romances sold 8 million combined copies
- By 1976 over 150 historical romance novels were published selling over 40 million copies

Two Types Of Romance

- **Category Romances** (series romances)
  - Short: 200 pages; 55,000 words; multiple books in a line published each month
  - “pare the story down to its essentials. Subplots and minor characters are eliminated or relegated ...”
  - Wide distribution, staying on shelves until sold out or until next month's titles arrive
- **Single-Title Romances**
  - Longer: 350-400 pages, 1/year, remain on shelves
  - Not always stand-alone, often Author-driven

Subgenres

- 40% Category Romance
- 17% Historical Romance
- 16% Contemporary Romance
- 9% Paranormal Romance
- 7% Romantic Suspense
- 6% Inspirational Romance
- 5% Other

Social Mores: Romance Novels 1980s

- 1980: WSJ refers to “bodice-rippers” as “publishing's answer to the Big Mac: they are juicy, cheap, predictable, and devoured in stupifying quantities by legions of loyal fans”
- Contemporary romances: weak females falling in love with alpha males
- Historical romances: heroines active in the plot, but “passive in relationships with heroes”
- All genres: heroines 16-21 virgins, heroes ~30 not, all are beautiful

The Sun Also Rises And Falls

- 1975: Harlequin purchases a romance novel that takes place in America with American morals
  - In the late 70's they reject Nora Roberts because "they already had their American writer"
- 1980: The Tawny Gold Man by Amii Lorin
  - First to waive the virgin heroine requirement
  - By 1983, sales of that line totaled $30 million
  - Similar lines soon had 90-100% monthly sellout rates
- 1984: Market Saturation (40% sellout rates)
  - "dampening effect of the high level of redundancy associated with series romances was evident in the decreased number of titles being read per month"

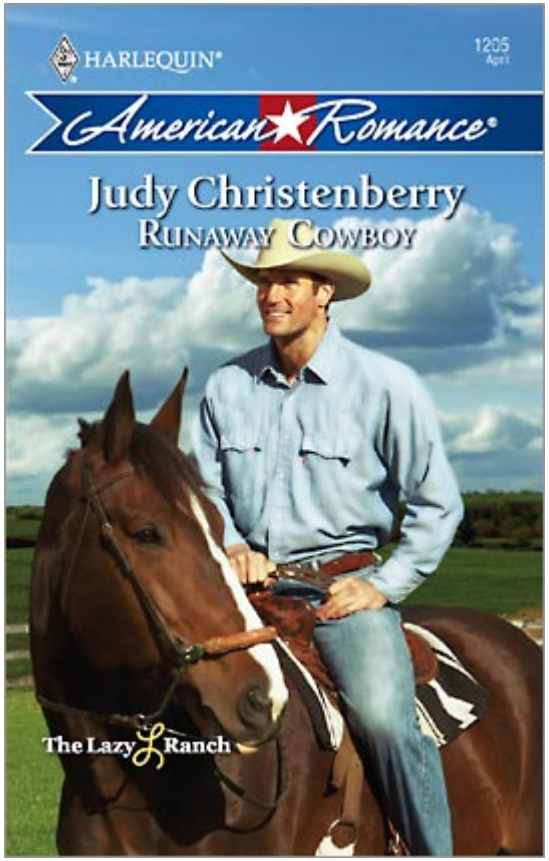
Social Changes

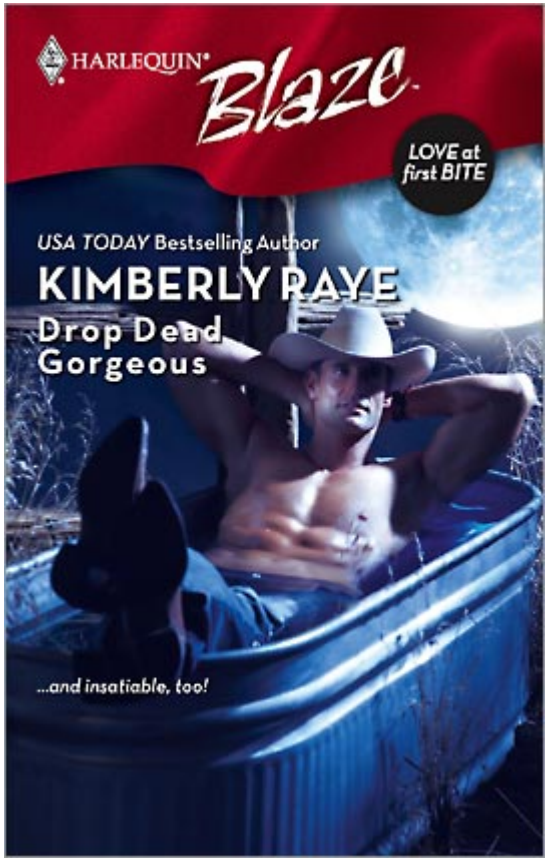
- 1984: overweight, middle-aged hero
- 1987: ugly hero, heroine searching for birth mother
- Late 1980's: heroines in more male-dominated jobs
- 1990's: self-employed heroines, 30-40 year old women, sensitive men
  - Later: single parenthood, adoption, abuse
  - Taboos: terrorism, warfare, masculine sports
- Now: what is **chick lit**?

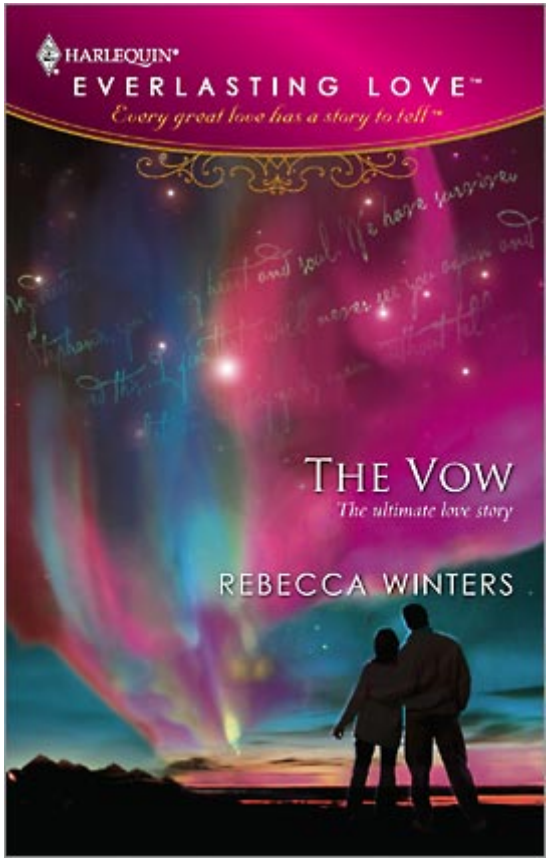
Category Romance

- Now the fun part ...
- I'll show you a bunch of different category romance lines
- You try to identify the **subgenre** and **target audience**

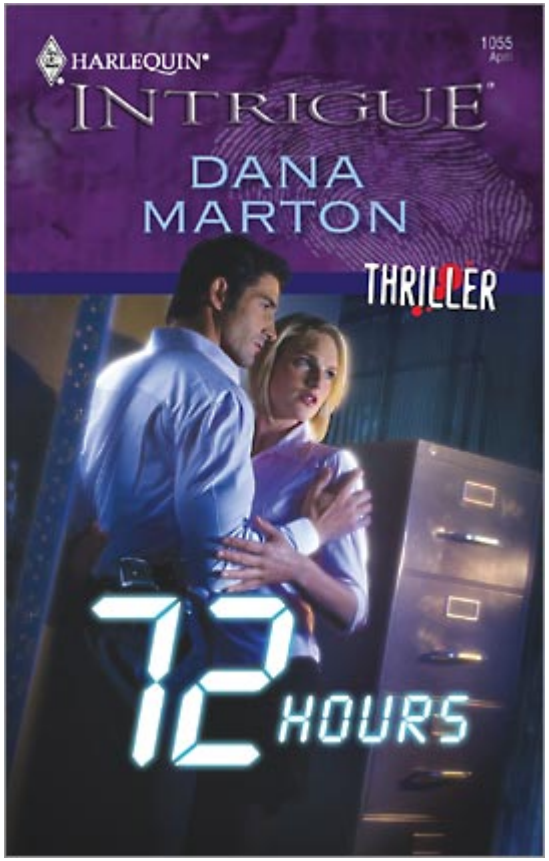
Category Romance In Pictures

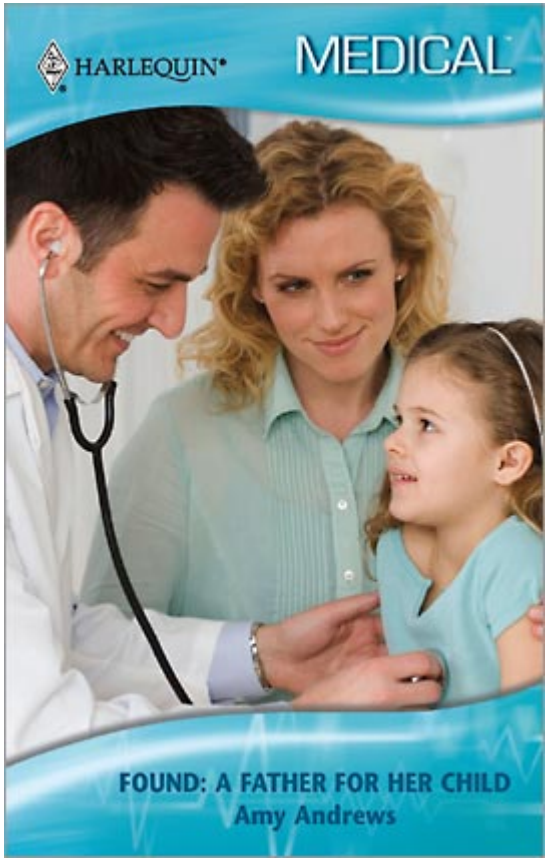


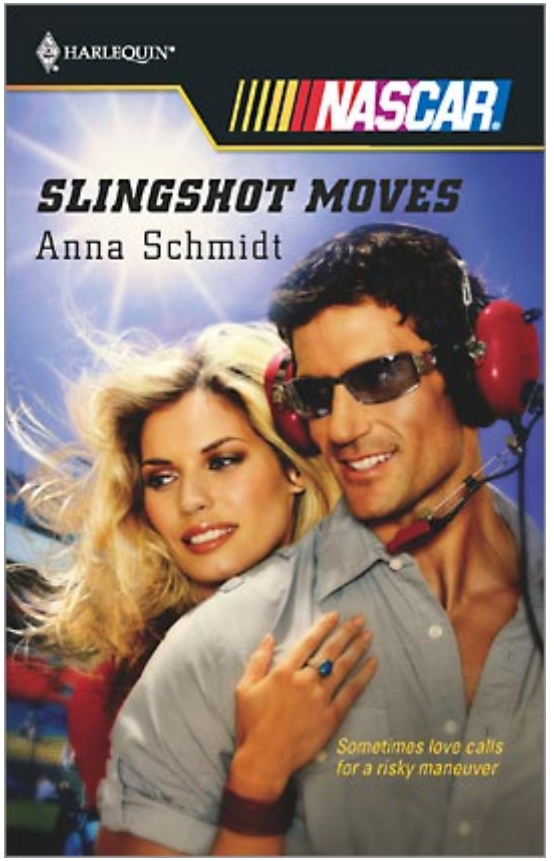




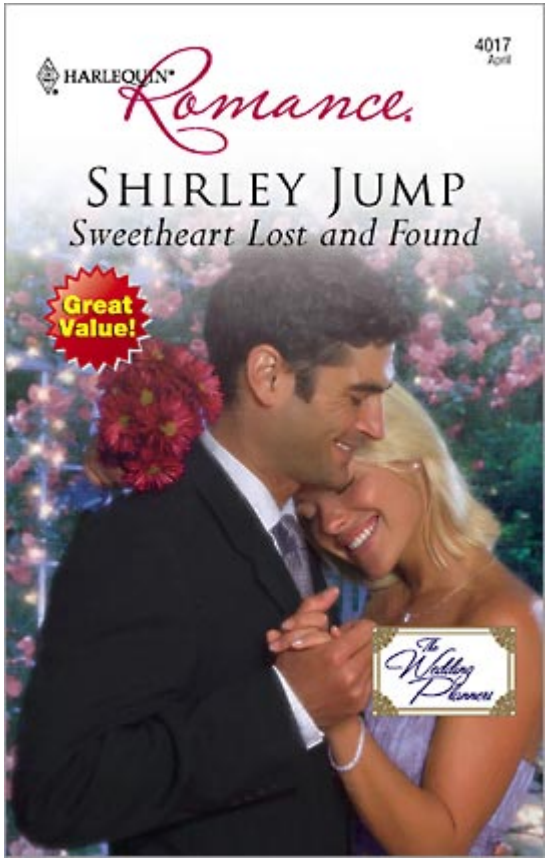
Category Romance In Pictures

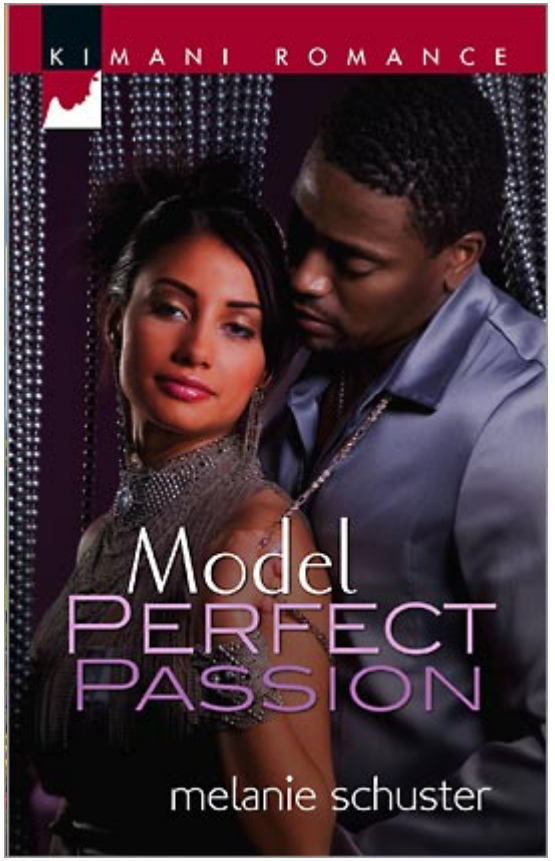


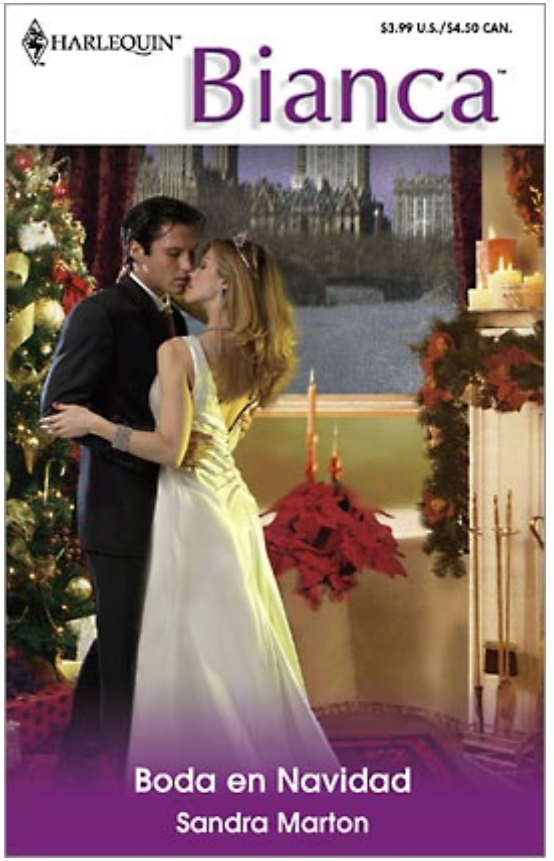




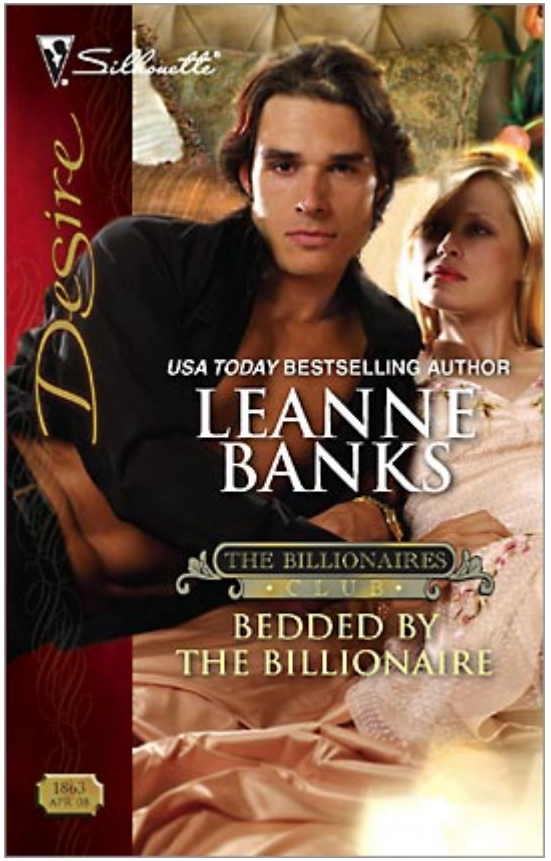
Category Romance In Pictures



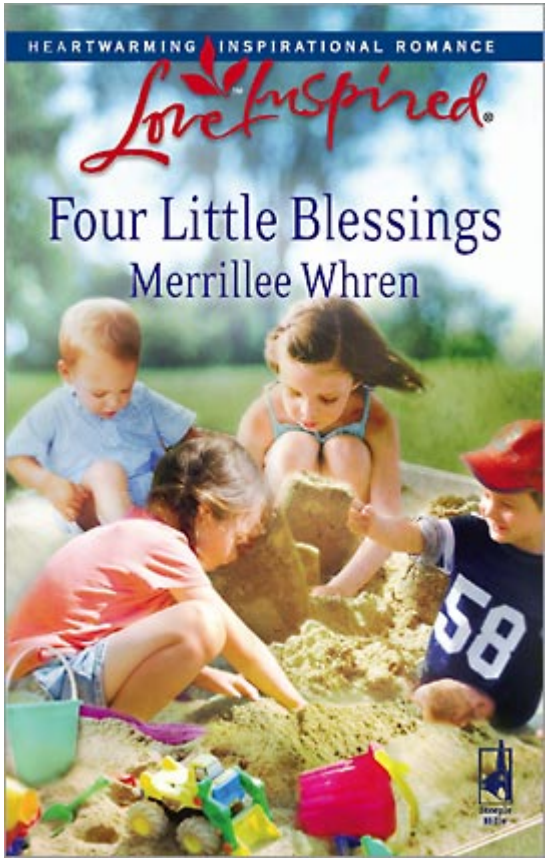


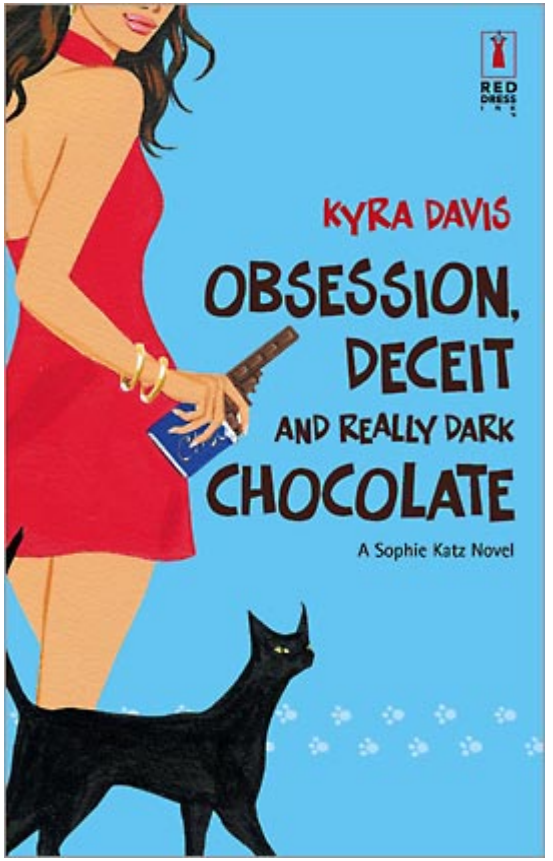


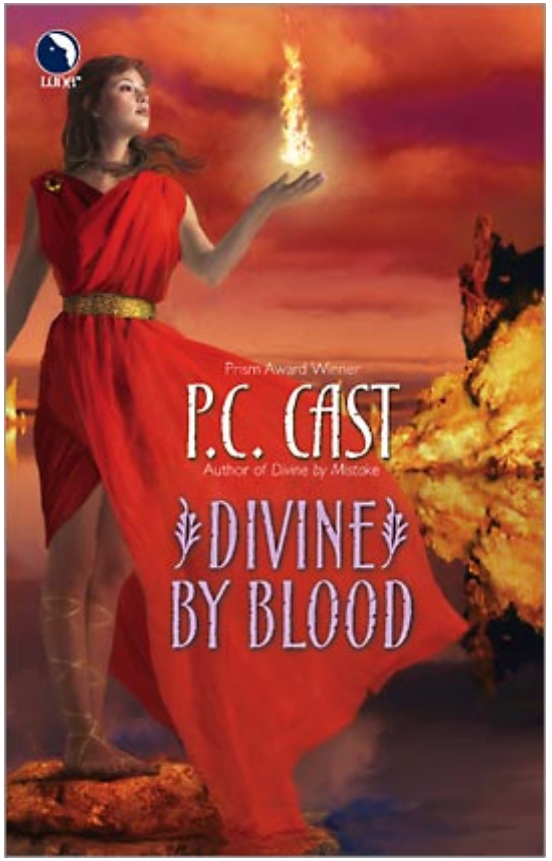
Category Romance In Pictures



Category Romance In Pictures







Conclusion

- Programming Languages is the topic of ultimate mastery
  - It combines rigorous theory
  - With the best parts of industrial practice
  - It is the cosmic mayonnaise that holds CS together
- This class is difficult (and also curved)
- Good job sticking it out!