Literature survey

- The aim of a literature review (sometimes called a literature survey) is to demonstrate to the reader that you have read and understood the main published work concerning a particular topic, and can summarise it, and objectively and critically review it.

Literature survey

- Due **Wednesday April 26th 2017 at 5pm** (but remember exam preparation)
- Can be about topic of your MSc Information Security dissertation
    - Cannot be copied into your dissertation, but will be a useful foundation
    - If dissertation is done by a pair, so can your survey
    - 20 pages (individual) or 35 pages (pair)
- Otherwise can be on topic of one paper presented in course

More on assessment and feedback for this course

- Submit slides and paper summaries by 10am on the day that the paper is to be presented
- General feedback will be provided during the lecture
- Marks and specific feedback will be sent to student **within 2 weeks** of the submission, using Moodle
- The student work and corresponding feedback will be made available to all class members on Moodle (but not the marks)
- Literature review will be submitted after the end of the course and feedback will be **within 4 weeks of submission** (24 May 2017) using Moodle

Marking criteria for this course (summaries, presentation and review)

- Understanding of paper(s) reviewed
- Background to the paper(s) including impact, contribution and context within the field
- Clarity of presentation
- Analysis of paper, including **(topic of this course)**
  - Appropriateness of methodology
  - Appropriateness of structure and presentation
  - Appropriateness of research design (e.g. experiments, quantitative or qualitative data)
  - Appropriateness of analysis techniques
  - Appropriateness of means to manage bias
  - Appropriateness of ethical considerations

Interpretation of assessment criteria and expectation

- Same rubric used for all coursework, which itself closely matches the one for the dissertation report
- Presentation and Summaries
  - Only the paper set needs to be discussed in detail but others will likely need to be briefly mentioned to properly discuss impact, context and contribution to the field
- Presentation
  - Clarity includes both slides and oral presentation
- Literature review
  - Much higher expectation for coverage of relevant literature in the field that is the topic of review, as well as critical analysis

Rubric for assessment

- Details on Moodle
- Mark will be average of *Understanding*, *Background*, *Clarity* and *Analysis* (25% each)
- Marks for each match upper mark for dissertation marking ranges: 100%, 89%, 79%, 69%, 59%, 49%, 44%, 29%, 0%
- If your work is within one of these ranges you get the upper limit as your mark
- **Positive marking used for coursework**, as with exams: starts at 0%; increases based on achievement)
- Not negative marking: starts at 100% and decreases based on any mistakes identified

Rubric on Moodle

Criteria		Scales								
		Exceptional 100.00	**Outstanding** 89.00	**Excellent (Distinction)** 79.00	**Good (Merit)** 69.00	**Satisfactory (Pass)** 59.00	**Borderline fail** 49.00	**Unsatisfactory** 44.00	**Unacceptable** 29.00	**Absent** 0.00
Understanding	25 %	Demonstrated exceptional understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped, creating a publishable contribution to the field	Demonstrated outstanding understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped, potentially creating a publishable contribution to the field	Demonstrated excellent understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	Evidence of understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	Some understanding of the paper(s) in terms of motivation, with main points mostly included and arguments grasped	Clear flaws in the understanding of the paper(s)	Some serious flaws in understanding	No proper evidence of understanding	No attempt
Background	25 %	Evidence of considerable background reading, mention of relevant literature, understanding of context, awareness of their impact, placing the work in the context of surrounding literature and identifying contribution of the	Evidence of background reading, mention of relevant literature, understanding of context, awareness of their impact, placing the work in the context of surrounding literature and identifying contribution of the	Demonstrated excellent understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	At least some awareness of the paper(s)' relevant and of identifying their contribution in the context of other literature	Limited awareness of the paper(s') relevant and of identifying their contribution	Clear flaws in the understanding of the paper(s)	Little or no understanding of related literature	No understanding of related literature	No attempt
Clarity	25 %	Close to faultless in execution and write-up in terms of organisation, use of citations, ease of understanding explanations, precise technical language	Only very minor faults in in terms of organisation, use of citations, ease of understanding explanations, precise technical language	Very well written with clear logical structure but some minor faults in execution of writing in terms use of citations, explanations, and/or precise technical language	Faults and ambiguities in execution of writing in terms use of citations, explanations, and/or precise technical language	Significant deficiencies in execution of writing in terms use of citations, explanations, and/or precise technical language	Substandard writing with noticeable errors or omissions in terms use of citations, explanations, and/or precise technical language, but could be made passable within a reasonable time	Somewhat incoherent rushed writing, containing important omissions, or irrelevant material	Writing is substantially absent, incomprehensible or wrong	No attempt
Analysis	25 %	Deep insight in critical analysis and added value e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Substantial insight in critical analysis and added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Good critical analysis and added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Reasonable level of critical analysis and some added value e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Adequate critical analysis has been demonstrated	Not quite enough critical analysis	Serious lack of critical analysis	No proper critical analysis	No attempt
Overall	0 %	This represents a really outstanding achievement. The coursework needs to clearly stand out above others. A mark in this range is hard to achieve and rare (< 1%)	Excellent in most respects but doesn't fully meet the criteria for the top range. A small number of coursework are in this range each year (2–3%)	This represents a straightforward distinction coursework. Most things have been done well but there will be some faults or criticisms. The goals have been met. A reasonable number of coursework can be expected to achieve this level	A good result, that is well on the way to meeting most criteria, but not completely so as to cover level of challenge. The majority of coursework are likely to be at this level	A satisfactory but limited coursework, attempts to meet the criteria are recognisable but are not complete. A minority of coursework are likely to be in this range (maybe 20%)	The coursework has enough substance to demonstrate it could be made into a pass in a fairly short length of time but it still significantly fails to meet the criteria	The basis of a viable coursework may be present but is a long way from meeting the criteria. A significant amount of additional work would be needed, to reach a passable standard	Really should never happen. A complete failure to engage and carry forward the coursework	No attempt

25%

25%

25%

0%

Rubric on Moodle

Distinction Merit Pass Fail

Criteria		Scales					
		Exceptional 100.00	**Outstanding** 89.00	**Excellent (Distinction)** 79.00	**Good (Merit)** 69.00	**Satisfactory (Pass)** 59.00	**Borderline fail** 49.00
Understanding	25 %	Demonstrated exceptional understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped, creating a publishable contribution to the field	Demonstrated outstanding understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped, potentially creating a publishable contribution to the field	Demonstrated excellent understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	Evidence of understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	Some understanding of the paper(s) in terms of motivation, with main points mostly included and arguments grasped	Clear flaws in the understa the paper(s)
Background	25 %	Evidence of considerable background reading, mention of relevant literature, understanding of context, awareness of their impact, placing the work in the context of surrounding literature and identifying contribution of the	Evidence of background reading, mention of relevant literature, understanding of context, awareness of their impact, placing the work in the context of surrounding literature and identifying contribution of the	Demonstrated excellent understanding of the paper(s) in terms of motivation, with main points included and appropriately weighted, arguments grasped	At least some awareness of the paper(s') impact; and of identifying their contribution in the context of other literature	Limited awareness of the paper(s') impact and of identifying their contribution	Clear flaws in the understar the paper(s)
Clarity	25 %	Close to faultless in execution and write-up in terms of organisation, use of citations, ease of understanding explanations, precise technical language	Only very minor faults in in terms of organisation, use of citations, ease of understanding explanations, precise technical language	Very well written with clear logical structure but some minor faults in execution of writing in terms use of citations, explanations, and/or precise technical language	Faults and ambiguities in execution of writing in terms use of citations, explanations, and/or precise technical language	Significant deficiencies in execution of writing, in terms use of citations, explanations, and/or precise technical language	Sub-standard writing with noticeable errors or omissi terms use of citations, expla and/or precise technical lan but could be made passabl a reasonable time
Analysis	25 %	Deep insight in critical analysis and added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Substantial insight in critical analysis and added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Good critical analysis and added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Reasonable level of critical analysis and some added value, e.g., new points not given by papers reviewed, errors in papers reviewed or identification of different approaches	Adequate critical analysis has been demonstrated	Not quite enough critical an
Overall	0 %	This represents a really outstanding	Excellent in most respects but	This represents a straightforward	A good result, that is well on the way	A satisfactory but limited	The coursework has enoug

Exceptional

- **90–100%** This represents a really outstanding achievement. The coursework needs to clearly stand out above others. A mark in this range is hard to achieve and rare (< 1%)

Outstanding

- **80–89%** Excellent in most respects but doesn’t fully meet the criteria for the top range. A small number of coursework are in this range each year (2–3%)

Excellent (Distinction)

- **70–79%** This represents a straightforward distinction coursework. Most things have been done well, but there will be some faults or criticisms. The goals have been met. A reasonable number of coursework can be expected to achieve this level (≈20%)

Good (Merit)

- **60–69%** A good result, that is well on the way to meeting most criteria, but not completely, or has a lower level of challenge. The majority of coursework are likely to be at this level

Satisfactory (Pass)

- **50–59%** A good result, that is well on the way to meeting most criteria, but not completely, or has a lower level of challenge. The majority of coursework are likely to be at this level

Borderline fail

- **45–49%** The coursework has enough substance to demonstrate it could be made into a pass in a fairly short length of time but it still significantly fails to meet the criteria

Unsatisfactory

- **30–44%** The basis of a viable coursework may be present but is a long way from meeting the criteria. A significant amount of additional work would be needed to reach a passable standard

Unacceptable

- **0–29%** Inexcusable result, that really should never happen. A complete failure to engage and carry forward the coursework

UCL plagiarism policy

"Any quotation from the published or unpublished works of other persons must, therefore, be **clearly identified as such by being placed inside quotation marks**, and students should identify their sources as accurately and fully as possible…

Under these Regulations students found to have committed an offence may be **excluded from all further examinations** of UCL or the University or of both."
http://www.ucl.ac.uk/current-students/guidelines/plagiarism

UCL plagiarism policy

- Plagiarism includes:
  - “turning in someone else's work as your own
  - copying words or ideas from someone else without giving credit
  - failing to put a quotation in quotation marks
  - giving incorrect information about the source of a quotation
  - changing words but copying the sentence structure of a source without giving credit
  - copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not”

http://www.ucl.ac.uk/current-students/guidelines/plagiarism

Feedback on talks and reviews: UCL plagiarism policy

- At minimum, plagiarised work cannot meet assessment criteria and **will result in a mark of zero**
- Don’t copy and paste text, even a phrase or sentence from papers for except quoting:
  - Inside quotation marks
  - With a reference to a bibliography at end
- Quotes should be there to support your own assertions, not as a substitution
- Generally quotes are not needed for presentations or paper reviews. Quotes may be needed for literature review
- Rules for figures are the same: include citation in caption

Dissertation projects

- Details on COMPGA99 Moodle on Tuesday 24 January, along with list of proposed projects and how to choose them
- Today there will be more presentations from some potential supervisors
- You need to submit your project preferences via Moodle by 7 February 2017

Principal Characteristics of Science

- Hypotheses
  - Falsifiable (hypotheses capable of being tested and refuted/supported)
- Logical deduction
- Objective observation:
  - Measurement and data (possibly although not necessarily using mathematics/statistics as a tool)
- Empirical evidence
- Experiment and/or observation as benchmarks for testing hypotheses

Source: Last three points - UK Science Council at http://www.sciencecouncil.org/definition

Principal Characteristics of Science

- Induction: reasoning to establish general rules or conclusions drawn from facts or examples
- Repetition (replicable results)
- Critical analysis
- Verification and testing: critical exposure to scrutiny, peer review and assessment
- Precision in data collection and analysis

Source: First four points - UK Science Council at http://www.sciencecouncil.org/definition

Principal Characteristics of Science

- Systematic/organised – argument can be followed from hypotheses to experimental findings, and through to conclusions – logical
- Controllable
- Defensible
- Contributes to body of scientific knowledge
- Findings are communicated
- Generalisable

A definition of science

- “Science is the pursuit and application of **knowledge** and **understanding** of the natural and social world following a **systematic methodology** based on **evidence**”

Source: UK Science Council at http://www.sciencecouncil.org/definition

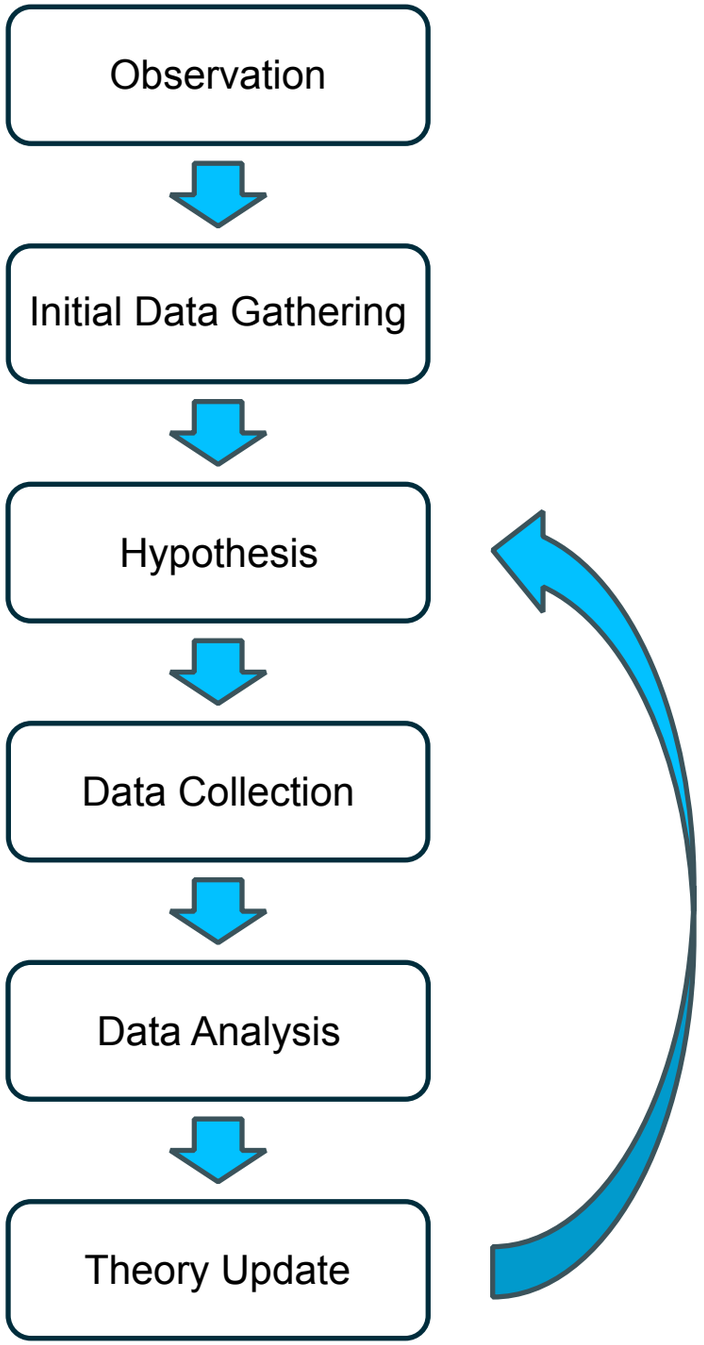
Demarcation Criteria

- The demarcation criteria
  - What is enough to distinguish genuine science from pseudoscience?
    - e.g. astrology, whilst generating a body of knowledge empirically, is not considered a genuine science
  - Why should astrology be seen differently from other sciences?
- Pseudoscience
  - Theories are compatible with all results
  - Does not recognise anything that its theories cannot explain
  - Is not falsifiable (Karl Popper)

Revolutionary Science

- Theory by Thomas Kuhn
- Normal science
  - Use of a paradigm to solve puzzles, with assumption that paradigm is incorrect
  - Anomalous results build up
- Paradigm shift
  - New paradigm which subsumes old results and anomalies (e.g. general relativity)

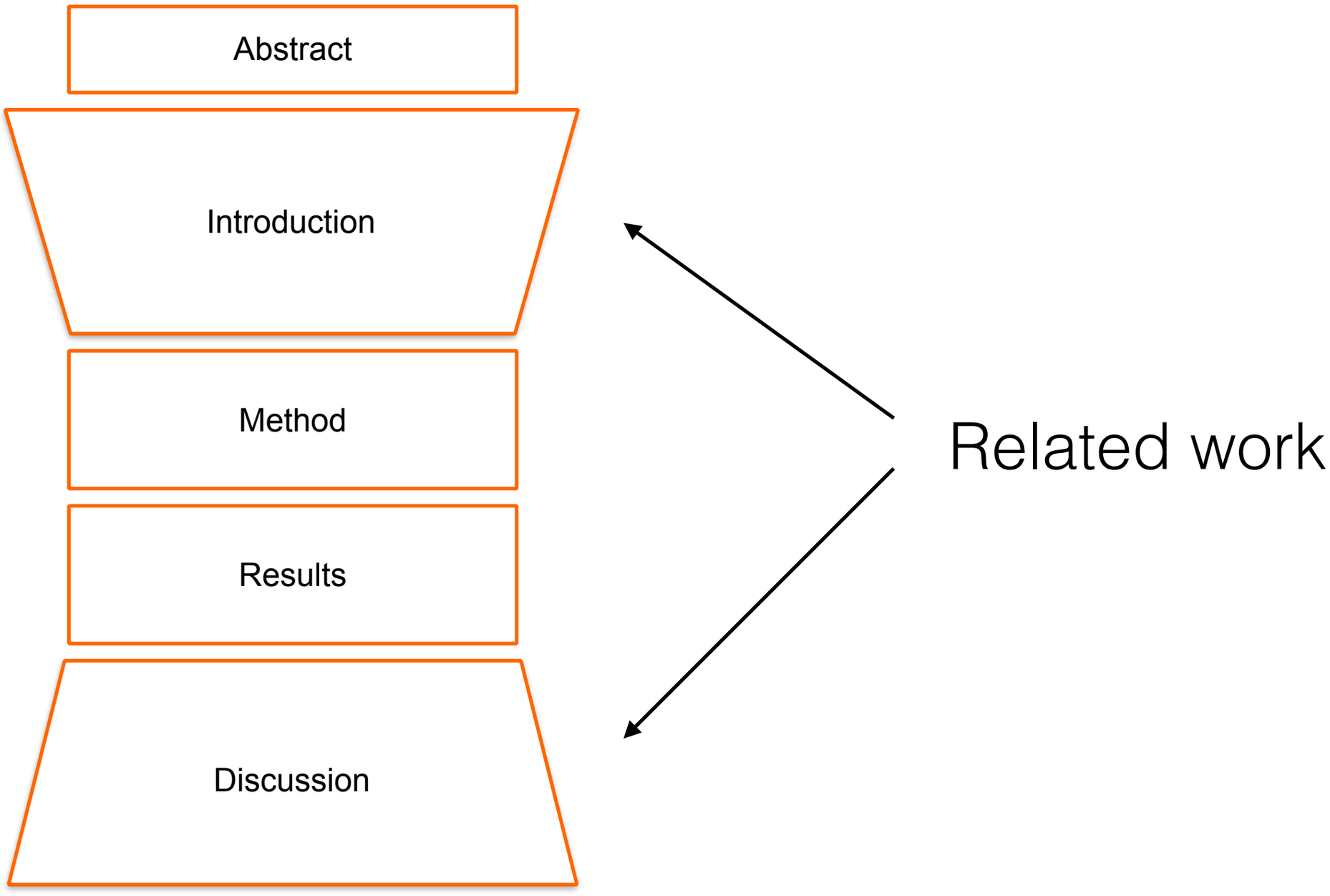
Scientific Method



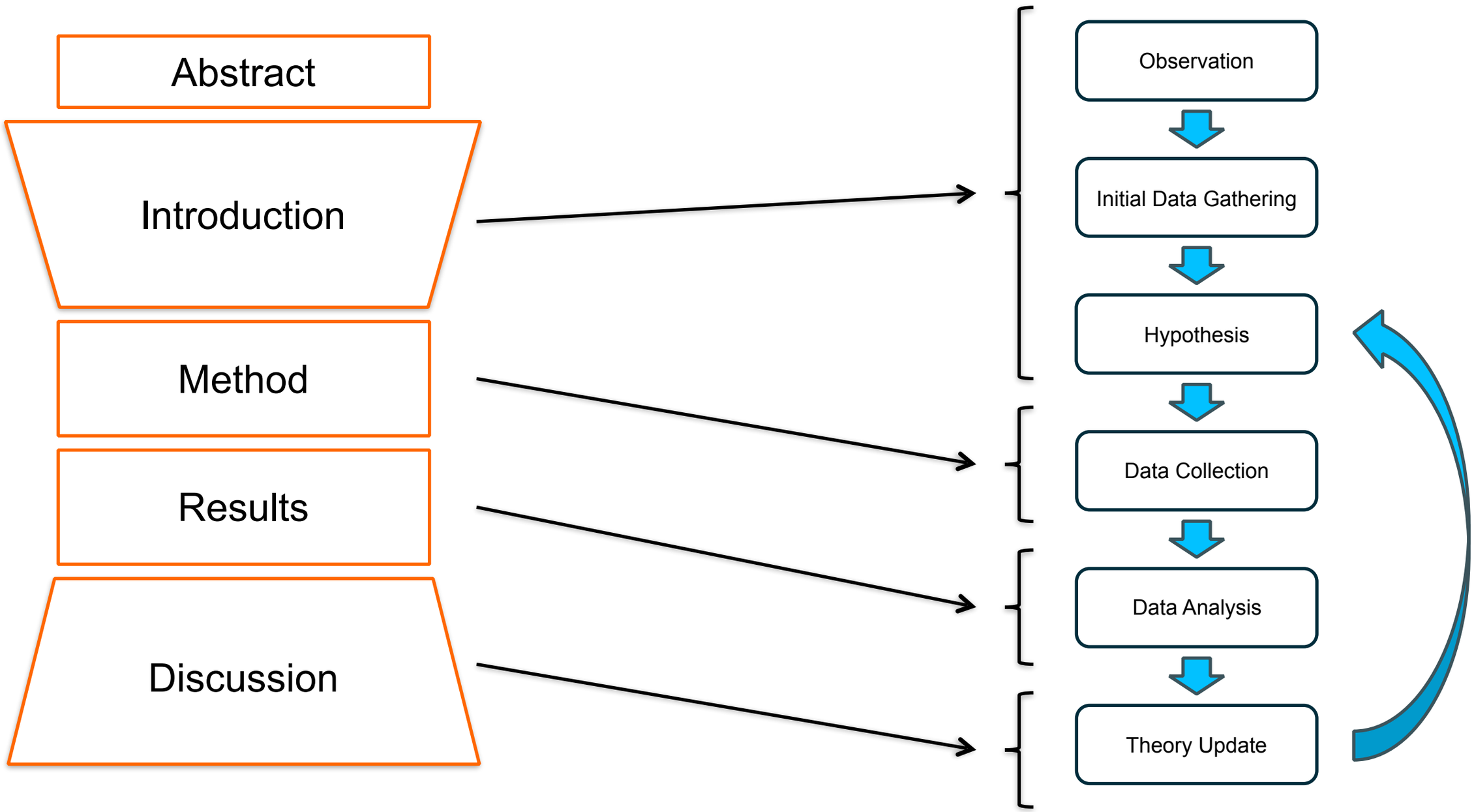
Scientific Paper

- Document written by researcher
- Usually describes a research study
- Goal is to communicate to other researchers:
    - objective;
    - methods; and
    - findings
- of the study
- May be written before and in-parallel to research

Typical structure

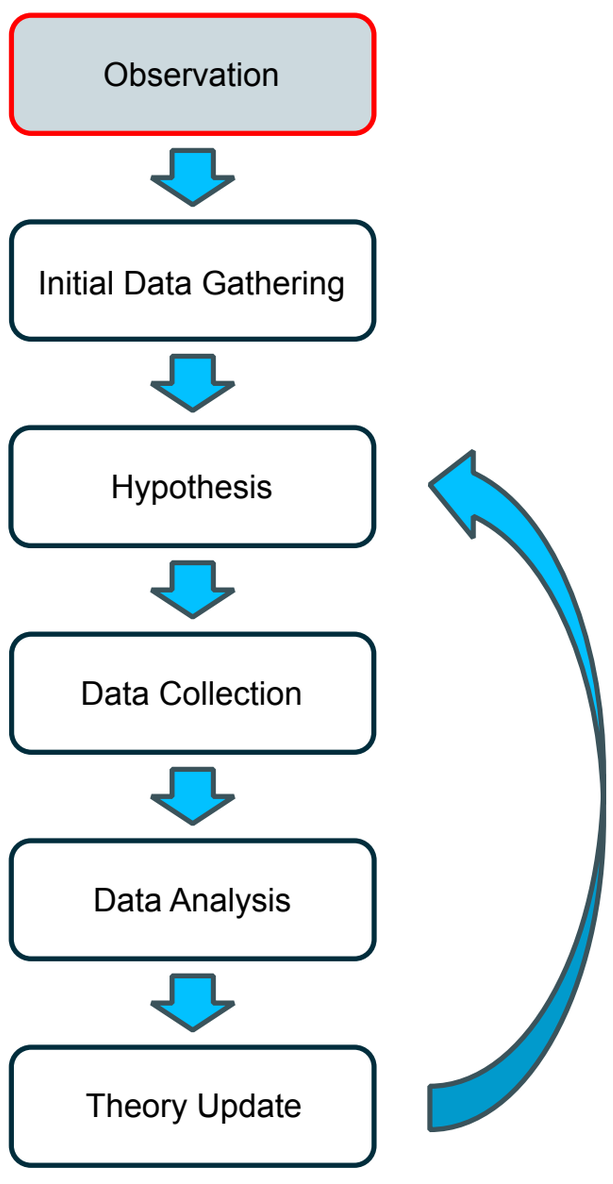


Scientific Method & Scientific Paper



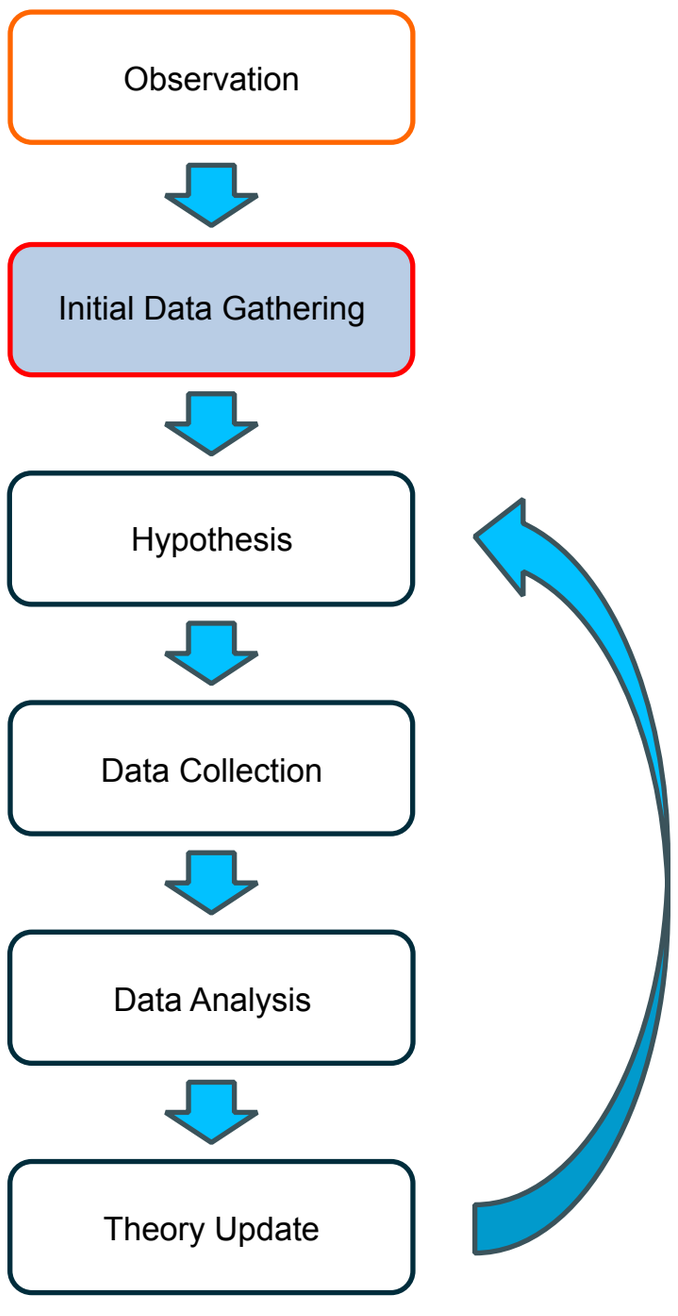
Observation

- Start by observing something you want to understand
  - Anecdotal
    - e.g. your friends tend to write their passwords on ‘post-it’ notes when they are complex, but not when they are simple
- Based on data
  - e.g. a diary study in an organisation revealed most employees write their passwords on ‘post-it’ notes



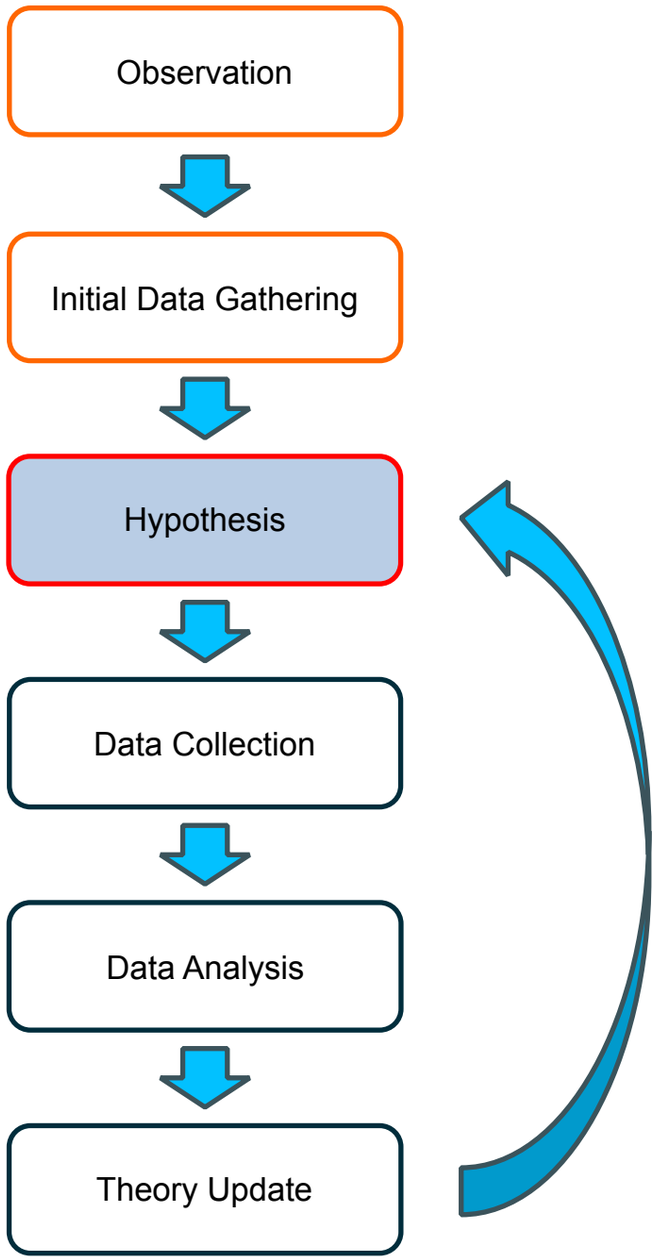
Initial Data Gathering

- Collect data to validate initial observation
  - Exploratory study collecting relevant variables
    - e.g. survey at organisation asking employees how frequently they write their passwords on ‘post-it’ notes
- Review of other research focused on same phenomena
  - journal articles, conference papers, PhD theses, etc.
  - Literature review



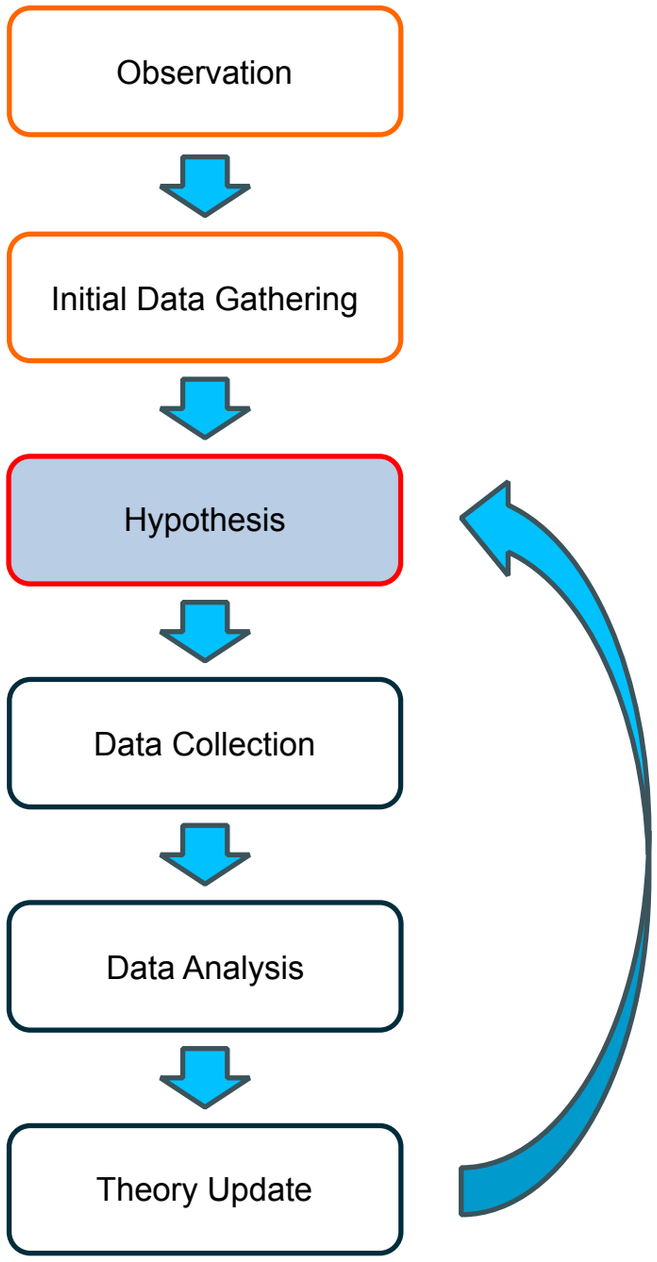
Hypothesis

- Attempts to explain observed phenomenon
  - e.g. password policies at organisations are too complex for employees to memorise
- Scientific hypotheses are empirically testable
  - e.g. the proportion of employees who write down their passwords is positively correlated with the complexity of the organisation's password policy



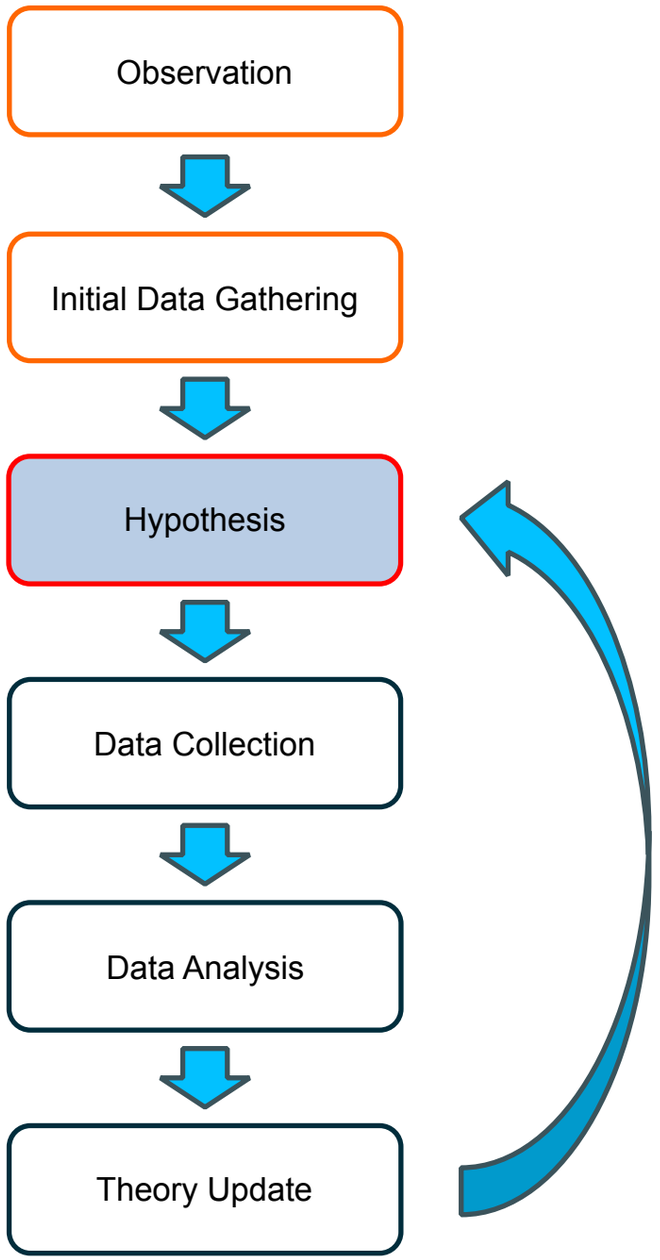
Hypothesis

- Scientific hypotheses
  - make predictions that can be disconfirmed by evidence
  - Popper's demarcation criteria: falsifiability
- Null hypothesis (H_0)
  - Reverse of experimental hypothesis
  - Represents default position where there is **no** relationship between the variables being observed
  - If data rejects H_0, then it gives support to experimental hypothesis
  - e.g. no correlation between password policies and proportion of employees writing passwords down



Hypothesis

- An untestable hypothesis is not a hypothesis
- Non-hypothesis:
  - e.g. “Citizen Kane is the best film ever”
- Hypothesis
  - e.g. “Avatar was the highest-grossing film of all time”



Hypotheses – Exercise 1

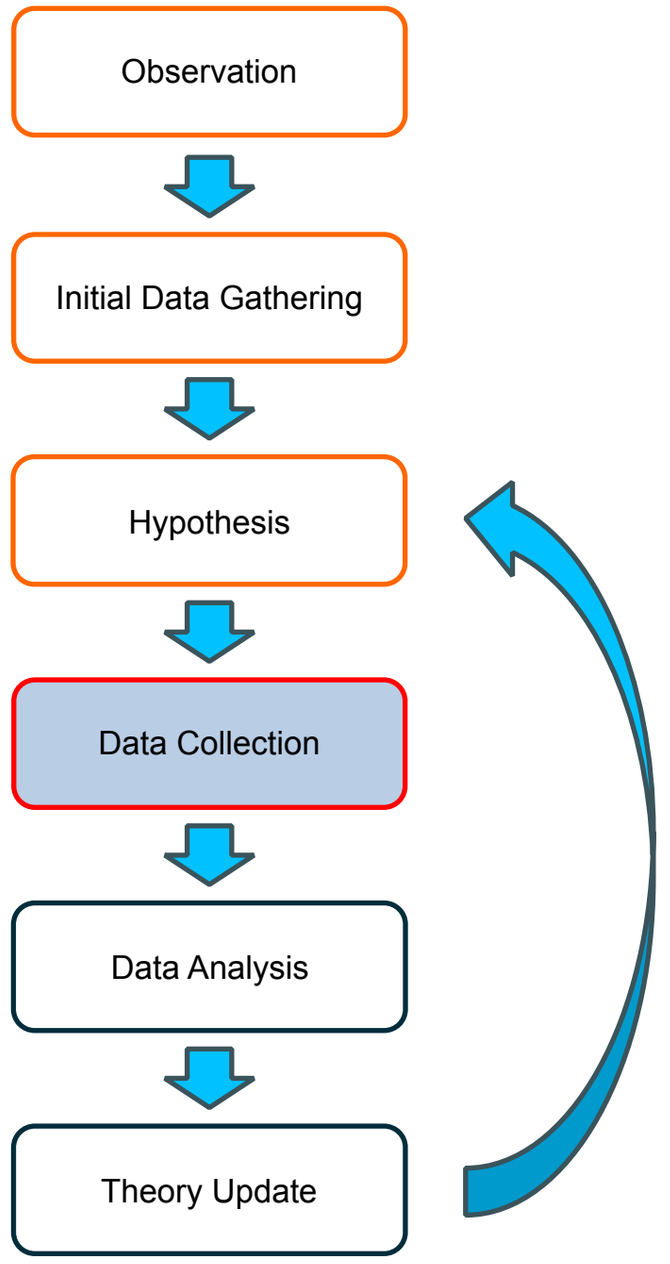
- Which of the following statements are hypotheses?
  - Longer passwords are more difficult to memorise.
  - The Beatles were the most influential band ever.
  - Facebook wants to control your personal data.
  - www.google.com is the web's most visited website.
  - My neighbour's internet connection is faster than mine.

Hypotheses – Exercise 2

- Suppose you make the following observations:
  1. There seems to be lots of shootings in countries with lots of guns and not that many shootings in countries with fewer guns;
  2. Your friends seem to post much more personal details on Facebook compared to your parents and their friends.
- Write a testable hypothesis based on each observation
  - What would the null hypothesis (H_0) be?

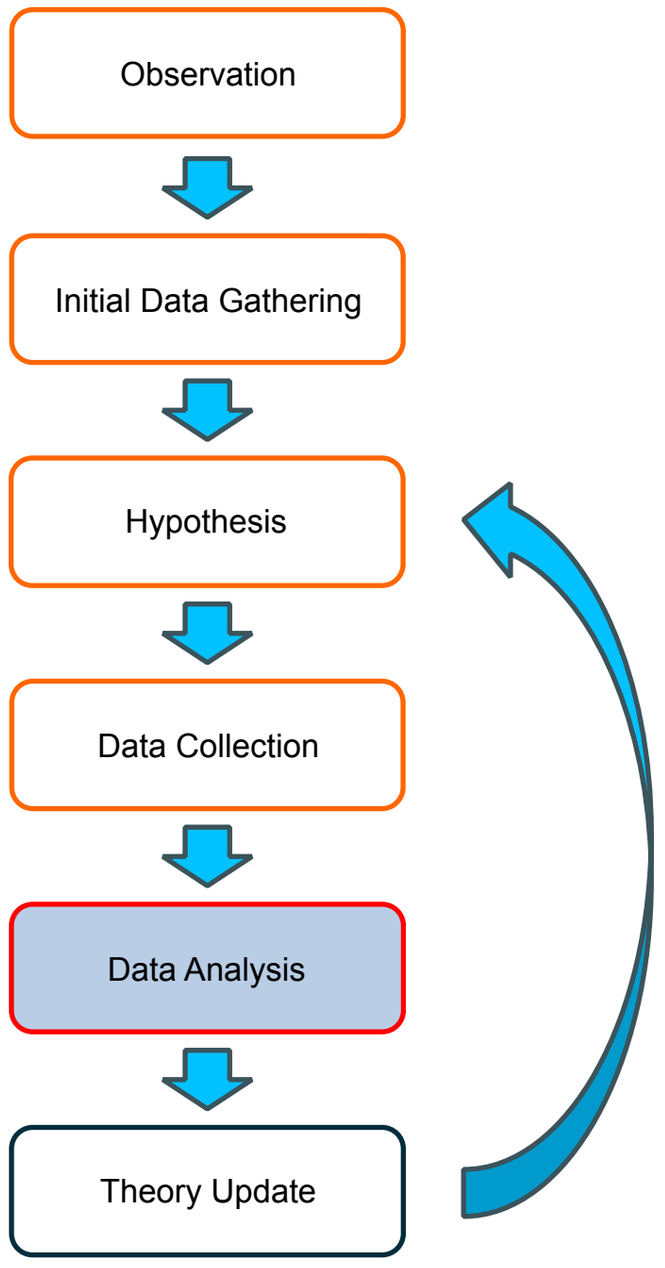
Data collection

- Collect data to test hypotheses
- What to measure
  - Independent variable (cause)
  - Dependent or outcome variable (effect)
- How to measure it
  - Correlational research (observation without interference)
  - Experimental research (manipulation of variables)



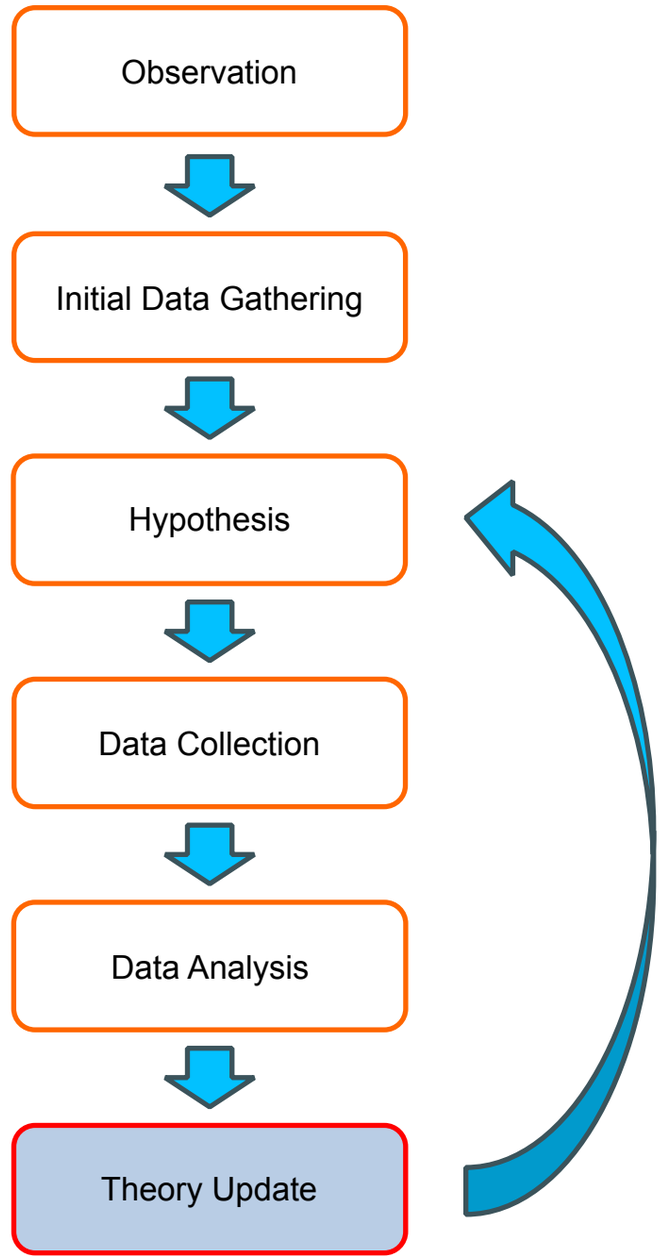
Data Analysis

- Quantitative data
  - Graphically representing the data
  - Fitting statistical models to the data
    - i.e. testing the null hypothesis
- Qualitative data
  - Thematic analysis
  - Grounded theory
- Very easy to confuse
  - Tip: think of “quantity”



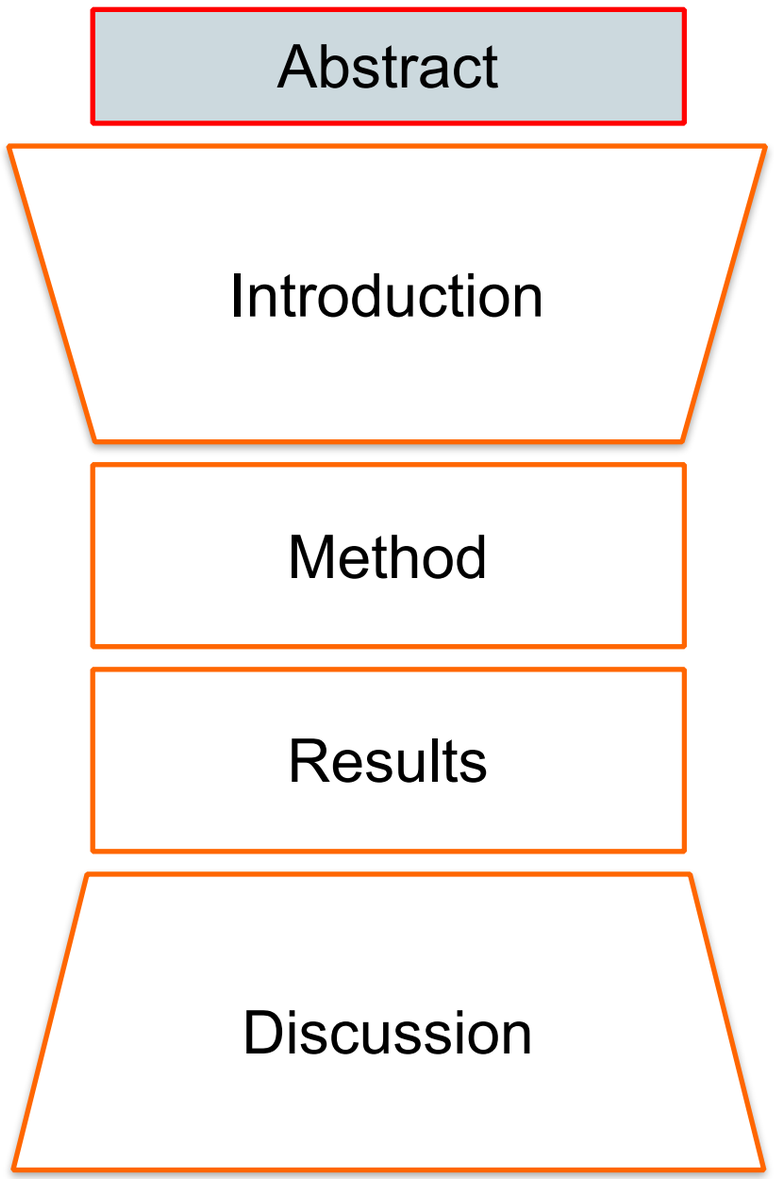
Theory Update

- Results of analysis may either:
  - support hypotheses; or
  - reject hypotheses.
- In case of rejection you may modify your theory
  - Generate new hypotheses
  - New research required to test new hypotheses



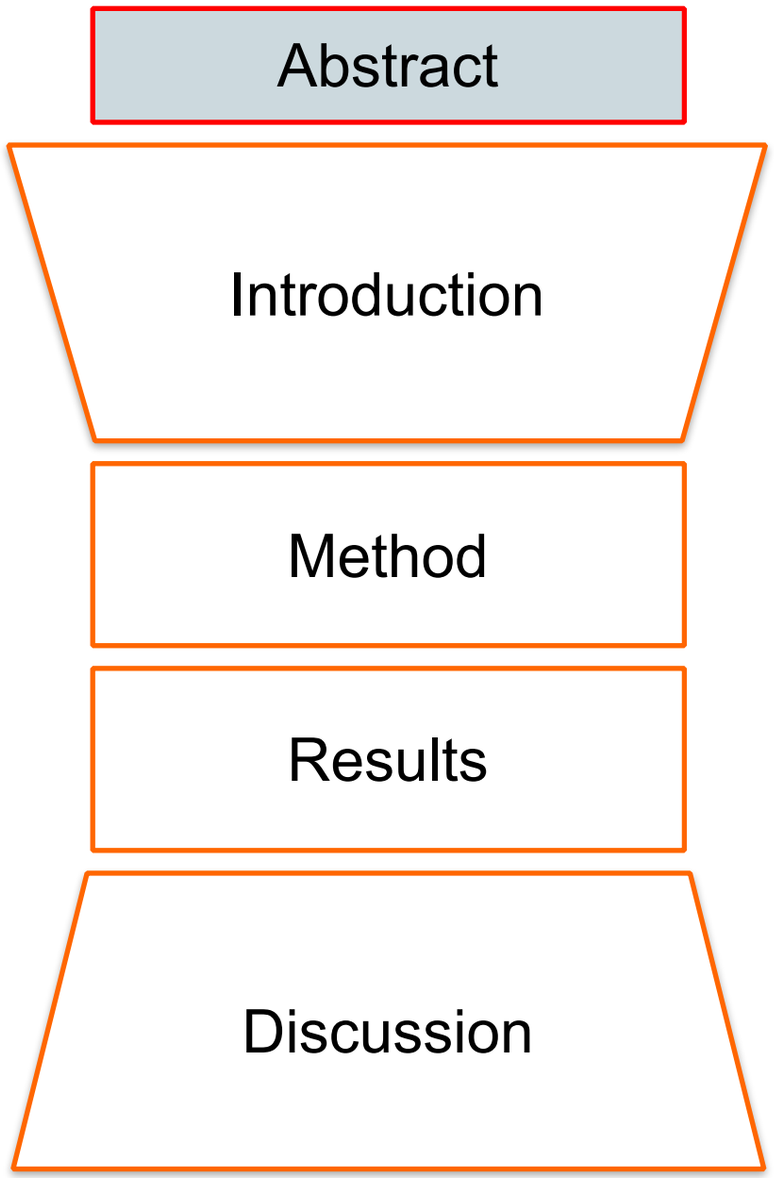
Scientific Paper - Abstract

- Brief summary of paper
  - Background information
  - Purpose of study
  - Methods
  - Most important findings
  - Conclusions and recommendations
- Includes elements from all sections



Scientific Paper - Abstract

- Usually last part to be written
- Readers will decide whether to read a whole paper based on it
- Very difficult to write
- Has a word limit
  - Usually 150 to 300 words



Example medical abstract

Drinking well water and occupational exposure to Herbicides is associated with chronic kidney disease, in Padavi-Sripura, Sri Lanka. Channa Jayasumana, Priyani Paranagama, Suneth Agampodi, Chinthaka Wijewardane, Sarath Gunatilake and Sisira Siribaddana. Environmental Health 2015, 14:6 doi:10.1186/1476-069X-14-6. Published: 18 January 2015

Background

The chronic kidney disease of unknown etiology (CKDu) among paddy farmers in was first reported in 1994 and has now become most important public health issue in dry zone of Sri Lanka. The objective was to identify risk factors associated with the epidemic in an area with high prevalence.

Methods

A case control study was carried out in Padavi-Sripura hospital in Trincomalee district. CKDu patients were defined using health ministry criteria. All confirmed cases (N = 125) fulfilling the entry criteria were recruited to the study. Control selection (N = 180) was done from people visiting the hospital for CKDu screening. Socio-demographic and data related to usage of applying pesticides and fertilizers were studied. Drinking water was also analyzed using ICP-MS and ELISA to determine the levels of metals and glyphosate.

Results

Majority of patients were farmers (N = 107, 85.6%) and were educated up to 'Ordinary Level' (N = 92, 73.6%). We specifically analyzed for the effect modification of, farming by sex, which showed a significantly higher risk for male farmers with OR 4.69 (95% CI 1.06-20.69) in comparison to their female counterparts. In the multivariable analysis the highest risk for CKDu was observed among participants who drank well water (OR 2.52, 95% CI 1.12-5.70) and had history of drinking water from an abandoned well (OR 5.43, 95% CI 2.88-10.26) and spray glyphosate (OR 5.12, 95% CI 2.33-11.26) as a pesticide. Water analysis showed significantly higher amount of hardness, electrical conductivity and glyphosate levels in abandoned wells. In addition Ca, Mg, Ba, Sr, Fe, Ti, V and Sr were high in abandoned wells. Surface water from reservoirs in the endemic area also showed contamination with glyphosate but at a much lower level. Glyphosate was not seen in water samples in the Colombo district.

Conclusion

The current study strongly favors the hypothesis that CKDu epidemic among farmers in dry zone of Sri Lanka is associated with, history of drinking water from a well that was abandoned. In addition, it is associated with spraying glyphosate and other pesticides in paddy fields. Farmers do not use personnel protective equipments and wears scanty clothing due to heat when spraying pesticides.

Example CS abstract

Secure Multiparty Computations on Bitcoin. Marcin Andrychowicz, Stefan Dziembowski∗, Daniel Malinowski, Łukasz Mazurek

Bitcoin is a decentralized digital currency, introduced in 2008, that has recently gained noticeable popularity. Its main features are: (a) it lacks a central authority that controls the transactions, (b) the list of transactions is publicly available, and (c) its syntax allows more advanced transactions than simply transferring the money. The goal of this paper is to show how these properties of Bitcoin can be used in the area of secure multiparty computation protocols (MPCs).

Firstly, we show that the Bitcoin system provides an attractive way to construct a version of "timed commitments", where the committer has to reveal his secret within a certain time frame, or to pay a fine. This, in turn, can be used to obtain fairness in some multiparty protocols. Secondly, we introduce a concept of multiparty protocols that work "directly on Bitcoin". Recall that the standard definition of the MPCs guarantees only that the protocol "emulates the trusted third party". Hence ensuring that the inputs are correct, and the outcome is respected is beyond the scope of the definition. Our observation is that the Bitcoin system can be used to go beyond the standard "emulation-based" definition, by constructing protocols that link their inputs and the outputs with the real Bitcoin transactions.

As an instantiation of this idea we construct protocols for secure multiparty lotteries using the Bitcoin currency, without relying on a trusted authority (one of these protocols uses the Bitcoin-based timed commitments mentioned above). Our protocols guarantee fairness for the honest parties no matter how the loser behaves. For example: if one party interrupts the protocol then her money is transferred to the honest participants. Our protocols are practical (to demonstrate it we performed their transactions in the actual Bitcoin system), and can be used in real life as a replacement for the online gambling sites. We think that this paradigm can have also other applications. We discuss some of them.