p 2q 6
RCJ

Professional Practice and Ethics

Computer Science Tripos 2002 - Part IA Exam
Solution Notes and Marking Scheme

20 point question (about 35 minutes)

Questions are in bold. The answers are taken from the lecture notes distributed during the course of the lectures.

Ethics

A. Characterize and distinguish between consequentialist ethical theories and deontological ethical theories. Give one example of each. (4 points)

Give one point each for a general characterization and for an example of each type of theory.

IV. Consequentialist Theories

Consequentialist theories are theories that determine moral values on the basis of their consequences. But the consequences are not confined to consequences for oneself but include consequences for everyone.

A. Utilitarian Theories and others

According to utilitarian theories we ought to do things which maximize pleasure or happiness for everyone, or, at least we should not interfere with people doing what gives them pleasure as long as it does not detract from the pleasure of others. A problem with this view is that not everyone makes pleasure or happiness their major goal. A more sophisticated version would aim to maximize satisfaction of preferences. But, even so, some people's preferences are not in their long term interests - children's food preferences, or drug addicts' preferences, for example.

B. Problems with Consequentialist Theories

There are a number of problems with consequentialist theories. First is the need to justify the basic claim that we ought to maximize pleasure (or happiness, or satisfaction of preferences). Second, there are real practical difficulties in quantifying happiness (or whatever). Third, there is no end to moral considerations - since every act has consequences, everything we do needs to be considered from a moral point of view. Fourth, such theories can lead us to treating certain individuals very badly if the total happiness is greater than their unhappiness.

V. Deontological Theories

An alternative way of answering the three basic ethical questions is to start from a consideration of what our duties are - irrespective of the consequences. One possible way of discovering our duties is through reason. Another is through considering our role in the social order.

A. Reason Based Theories

1. Kant

Kant argued that some moral principles were rational. Kant's ethics is based on the 'Categorical Imperative': Act only on the maxim which you can at the same time will to be a universal law. This principle can be used to justify the principle of telling the truth because if we considered the principle 'lie when it is convenient' the institution of truth-telling would collapse and it would no longer be possible to lie.

2. Natural Rights

In a state of nature we are free to do whatever we want. Some of these freedoms we can agree to compromise in the interest of social accord, but others are too basic to compromise. The freedom to gather in groups and to speak together, for example, are necessary to achieving such agreements and social accord and therefore cannot be compromised. Other freedoms, such as the freedom to take what we want from what we see around us or the freedom to kill those whom we don't like, can be given up in the interest of social accord.

C. Contract Theories

An increasingly popular method for determining and justifying moral values is to consider what principles contribute to a fair and harmonious social order.

1. Egoistic Contract Theory

From the egoistic point of view it is in our own interest to make some agreements with other people around us to refrain from certain kinds of actions like stealing and killing. But this depends on an equal distribution of power - if we can act against others and prevent them from acting against us, then we are justified in acting against them.

2. Rawls' Theory of Justice

Social contract theories suppose that our duties are determined by an agreement that we make with others in order to further our own personal goals. But in fact we are born into an existing social practice. For John Rawls the justice of a given practice can be analyzed by considering whether we would be satisfied to be born into any role in that practice. We may wonder if it is really possible to put aside our interests and look at a social practice through a "veil of ignorance".

Professions

B. The first section of the new British Computer Society Code of Conduct sets out for BCS professionals six standards of how they should conduct themselves with respect to The Public Interest. State four of these standards. (4 points)

Give one point for each correctly stated standard up to four.

The Public Interest

1. You shall carry out work or study with due care and diligence in accordance with the relevant authority's requirements, and the interests of system users. If your professional judgement is overruled, you shall indicate the likely risks and consequences.
   - The crux of the issue here, familiar to all professionals in whatever field, is the potential conflict between full and committed compliance with the relevant authority's wishes, and the independent and considered exercise of your judgement.
   - If your judgement is overruled, you are encouraged to seek advice and guidance from a peer or colleague on how best to respond.
2. In your professional role you shall have regard for the public health, safety and environment.
   - This is a general responsibility, which may be governed by legislation, convention or protocol.
   - If in doubt over the appropriate course of action to take in particular circumstances you should seek the counsel of a peer or colleague.
3. You shall have regard to the legitimate rights of third parties.
   - The term 'third Party' includes professional colleagues, or possibly competitors, or members of 'the public' who might be affected by an IS project without their being directly aware of its existence.
4. You shall ensure that within your professional field/s you have knowledge and understanding of relevant legislation, regulations and standards, and that you comply with such requirements.
   - As examples, relevant legislation could, in the UK, include The UK Public Disclosure Act, Data Protection or Privacy legislation, Computer Misuse law, legislation concerned with the export or import of technology, possibly for national security reasons, or law relating to intellectual property. This list is not exhaustive, and you should ensure that you are aware of any legislation relevant to your professional responsibilities.
   - In the international context, you should be aware of, and understand, the requirements of law specific to the jurisdiction within which you are working, and, where relevant, to supranational legislation such as EU law and regulation. You should seek specialist advice when necessary.
5. You shall conduct your professional activities without discrimination against clients or colleagues
   - Grounds of discrimination include race, colour, ethnic origin, sexual orientation
   - All colleagues have a right to be treated with dignity and respect.

- You should adhere to relevant law within the jurisdiction where you are working and, if appropriate, the European Convention on Human Rights.
- You are encouraged to promote equal access to the benefits of IS by all groups in society, and to avoid and reduce 'social exclusion' from IS wherever opportunities arise.

6. You shall reject any offer of bribery or inducement.

Cracking

C. Computer security is as much a matter of institutional safeguards as it is of technical safeguards. Explain the two main aspects of institutional safeguards. (2 points)

The two are institutional structure and institutional control, but they need to be explained. If the explanation is correct and the labels are wrong give the points anyway.

5. Institutional Safeguards

Whatever attitudes and laws might be in place to guard against computer cracking, there will still be those who find it a challange, and others who can use the craft of cracking as the basis for criminal activity. For this reason technical security - passwords, encryption, etc. - will be needed to protect sensitive information. But such security will have no value if institutional safeguards are not in place. There are two aspects of institutional safeguarding that require attention. The first is the institutional structure - There should be clear rules about who has access to what information and the responsibility for access should be well defined. The second is institutional control - once the institutional structure is in place it should be adhered to, those with access to sensitive information should know what their responsibilities are and should take care that the security of the system is not compromised through neglegence on their part.

(C) Name two new offences created by the Computer Misuse Act of 1990. (2 points)

Any two of I, II or III below will do. A and B score half a point each.

a. The Computer Misuse Act of 1990

On 10 October 1989 the Law Commission recommended legislation on the problem of computer abuse. Their recommendations were essentially adopted in the *Computer Misuse Act 1990*, which became law in June 1990. The law creates three new offences:

I. Unauthorised entry into a computer system, with a maximum penalty of £2,000 fine or six months' imprisonment (the Law Commission suggested a maximum penalty of three months imprisonment)

II. Unauthorised entry with intent to commit or assist in serious crime, with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission suggested a maximum penalty of five years' imprisonment)

III. Altering computer-held data or programs without authorisation, also with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission again suggested a maximum penalty of five years' imprisonment)

Two extensions of this basic law should be noted:

A. The law is extended to cover those who conspire with others to break the law and those who incite others to break the law.

B. The law applies to any violation of the law which has a significant link in the UK. For example misusing a computer in Italy through an ftp connection in the UK is breaking the law. Also if the culprit is not in the UK but accesses the Italian computer through a link in the UK they are guilty of breaking this law.

Privacy

D. State as accurately as you can four of the eight principles of the 1998 Data Protection Act and briefly explain the reason for having each of these principles. (4 points)

1. First Principle (principle of data gathering)

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The basic condition for a) is that the subject has given consent for their data to be processed, but there are a number of exceptions such as processing that is required for performance of a contract to which the subject is party, and processing that is required by the government. The "sensitive personal data" of clause b) includes data on such things as the racial or ethnic origin of the data subject, their political opinions, their religious (or similar) beliefs, their sexual life, and their criminal record.

Under the DPA of 1998 the subject must at least actively consent to having personal data gathered (e.g., failure to return or respond to a leaflet does not count as consent) and where the data is more sensitive they must explicitly consent to having the data processed (i.e., write it down).

The First Principle also subsumes two other important aspects of personal control of data - the right of the data subject to know what personal data is being gathered (the old OECD openness principle) and the uses to which that data is being put (the old OECD purpose specification principle).

The OECD purpose specification principle appeared as principle 2 of the UK DPA of 1984. In the DPA of 1998, purpose specification is included in the principle of fair and lawful processing. In particular, this first principle contains a fair processing code which specifies the information to be provided to data subjects. In addition to the identity of the data controller, the data subject must be told the purpose for which the data are to be processed. But the requirements do not stop here - the data subject must also be informed of the likely consequences of such processing and especially whether disclosure of such information can reasonably be envisaged. In particular the data processor is obliged to inform the subject of consequences of processing that the subject may not forsee.

The OECD openness principle held that the data subject should be able to determine the whereabouts, use and purpose of personal data relating to them. The availability of this kind of information creates its own problems of security. We can imagine files which hold personal data about individuals who do not object to having that data held, but who would object to other people knowing that that data is held. For example, police records, or hospital records of people who are HIV positive, or building society records of people who have had to renegotiate their mortgages because of financial hardship. In such cases it would be a breach of privacy if someone else could discover the whereabouts, use and purpose of personal data relating to them. A central register of individuals and the files which included them would then itself require a high degree of security and pose a potential threat to privacy. For this reason no central register is kept, and the openness principle is reduced to the rights of data subjects covered by the sixth principle.

2. Second Principle (principle of data quantity)

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Third Principle (principle of data quantity)

Personal data shall be adequate, relevant and not excessive in relation to the purposes or purposes for which they are processed.

4. Fourth Principle (principle of data quality)

Personal data shall be accurate and, where necessary, kept up to date.

5. Fifth Principle (principle of data lifetime)

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Sixth Principle (principle of data subjects' rights)

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The first right of the data subject is to be told by any data processor if their own personal data is being processed and, if it is, to be told in an intelligible manner what that personal data is, the purposes for which it is being processed, and to whom the personal data may be disclosed.

The data subject also has the right to prevent processing for purposes of direct marketing or where the processing is likely to cause damage or distress, and the data subject has the right to seek a court order requiring the data controller to rectify, block, erase or destroy inaccurate data.

Finally, the data subject has the right to seek compensation for any damage or distress that may result from contravention of the act.

7. Seventh Principle (principle of data security - internal)

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Eighth Principle (principle of data security - external)

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The act is enforced through the office of the Data Protection Registrar (DPR) who maintains a register of data collectors and processors. Individuals and organizations who regularly process personal data are legally obliged to register themselves with the DPR. They must state what kind of data they are processing and for what purpose they are using it. They are breaking the terms of the DPA if they use the data for any other purpose than what is stated. In addition to the penalties that may have to be paid to individuals if damage is done through misuse of personal data, the data processor can be struck off the register of data collectors and processors. If he is struck off the record then it is illegal for him to store or process any electronic personal data.

Property

E. What is the difficulty in trying to claim that people have natural rights to the ownership of intellectual property such as software? Is there a consequentialist justification for maintaining ownership of intellectual property such as software? (4 points)

One point for stating a case for natural rights of ownership, one point for saying how this doesn't work for intellectual property, one point for giving the consequentialist justification and one point for providing a reply to this.

B. The Basis of property law

To try to resolve and clarify questions about possession of software it is worth considering how laws of property are justified in the first place. Traditionally there are two ways in which we can try to justify laws of property. We can try to justify them on the basis of a natural right of ownership, or we can try to justify them on the basis of their consequences.

1. Natural rights

a. The argument for ownership

The justification of ownership based on natural rights appeals to the idea that a person has a natural right to possess what she produces. The labour that she puts into her production is hers to begin with and thus the product of her labour should remain hers. The product would not have existed without her labour, it is composed, at least in part, of her labour. As such it should remain hers, she has a right to own it.

b. Replies

In the case of software this argument seems to miss the point. If the product of a person's labour is a programme, then she still has it even if someone copies it. If I make a pot out of clay from the common, and you take it from me, then I don't have it any more. But if I write a programme and you copy it out of my files I still have it. So why do I object to your taking it in this way? The only objection can be in terms of some advantage I might gain by having exclusive use of it, in particular the financial advantage I gain by selling it. But we can imagine a world where software never enters the commercial realm? We can easily imagine a world where software is published like scientific articles and the writer is rewarded in the same way as scientists are rewarded for their publications. In this world we would be highly motivated to publish our software. It seems that the morality of software ownership depends on the social system in which we live. In other words, software ownership, at least, seems not to be a natural right.

2. Consequences

a. The argument for ownership

The central motivation for maintaining the right to own software is the profit motive, and this is justified on the grounds that innovation will only come about if there is some advantage to be gained. On this basis, the right to own software is not a natural right but a social right that is justified in terms of its beneficial social consequences. The socially desirable consequences are progress and development of software. This progress and development, it is argued, will not take place unless those who make the effort to bring it about can see something in it for themselves. And that, it is claimed, is profit. The only way to guarantee profit for the producers of software is to give them control over the use and distribution of the software. They can then sell or license it for whatever profit they can get. It is argued that this system has the advantage that quality will be maximized through competition in the marketplace. Software of higher quality will naturally attract higher profits and so the sellers of software will strive to improve their software. This is the consequentialist argument for the social right to ownership.

b. Replies

In the early days of computing people developed software without the profit motive. The motive then was interest, curiosity, intellectual challenge, and, of course, need. Those who created useful software were rewarded within the computer community by the respect and appreciation of those who where able to benefit from the use of the software. In science this is still the prevailing way in which good work is rewarded. Publication of scientific work is the hallmark of success, the work is then available to the scientific community to use and build on as it sees fit. It is not hard to imagine a similar kind of reward system being used in the production of software. Of course if software developers were not to take their income from the marketplace, they would require another source of income. Funding for software developers would have to come from another source. In science this comes from government spending on universities and through research councils. And it is not impossible to imagine a similar source of funding for software developers. But this would depend on further government spending and thus on the political climate. If the political climate favours private sector enterprise, then the science model of software development will not work.