Resilience of Machine Learning Applications against Hardware Faults

from Safety and Security Perspective

by

Michael M^{c}Neil Forbes

B.Sc., The University of British Columbia, 1999
M.Sc., The University of British Columbia, 2001
Ph.D., Massachusetts Institute of Technology, 2005

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate Studies

(Physics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2021

Abstract

The `genthesis.cls` LaTeX class file and accompanying documents, such as this sample thesis, are distributed in the hope that it will be useful but without any warranty (without even the implied warranty of fitness for a particular purpose). For a description of this file's purpose, and instructions on its use, see below.

These files are distributed under the GPL which should be included here in the future. Please let the author know of any changes or improvements that should be made.

Michael Forbes. mforbes@physics.ubc.ca

Preface

You must include a preface if any part of your research was partly or wholly published in articles, was part of a collaboration, or required the approval of UBC Research Ethics Boards.

The Preface must include the following:

- A statement indicating the relative contributions of all collaborators and co-authors of publications (if any), emphasizing details of your contribution, and stating the proportion of research and writing conducted by you.
- A list of any publications arising from work presented in the dissertation, and the chapter(s) in which the work is located.
- The name of the particular UBC Research Ethics Board, and the Certificate Number(s) of the Ethics Certificate(s) obtained, if ethics approval was required for the research.

Examples

Chapter 7 is based on work conducted in UBC's Maple Syrup Laboratory by Dr. A. Apple, Professor B. Boat, and Michael McNeil Forbes. I was responsible for tapping the trees in forests X and Z, conducted and supervised all boiling operations, and performed frequent quality control tests on the product.

A version of chapter 7 has been published [**?**]. I conducted all the testing and wrote most of the manuscript. The section on "Testing Implements" was originally drafted by Boat, B. Check the first pages of this chapter to see footnotes with similar information.

Note that this preface must come before the table of contents. Note also that this section "Examples" should not be listed in the table of contents, so we have used the starred form: `\section*{Example}`.

Table of Contents

Abstract ii

Preface iii

Table of Contents iv

List of Tables vi

List of Figures vii

List of Programs viii

Acknowledgements ix

Dedication x

1 Background and Terminology 1

2 Protecting Quantized CNNs against Rowhammer through Adversarial Training 2

3 Measuring Fault Resilience of CNNs against Weight Faults 3

4 Some Parameters are more Equal 2

5 Abstract 3
5.1 Experimental Setup 4
5.2 Results 4

6 This is a Chapter 7
6.1 A Section 7
6.1.1 This is a Subsection 7
6.2 Quote 9
6.3 Programs 9

7 Another Chapter... 11
7.1 Another Section 11
7.2 Tables 13

8 Landscape Mode 16

Appendices

A First Appendix 18

B Second Appendix 19

List of Tables

6.1 Here is the caption for this wonderful table. 8

7.1 Another table. 13
7.2 Feasible triples for highly variable Grid 13

List of Figures

5.1 Performance of heuristics in comparison to random parameter selection. Including injections to all layers. 5
5.2 Performance of heuristics in comparison to random parameter selection. Excluding the injections to the last layer. 6

7.1 Happy Face: figure example. 12

List of Programs

6.1 Python program that computes the n^{th} Fibonacci number using memoization. 10

Acknowledgements

This is the place to thank professional colleagues and people who have given you the most help during the course of your graduate work.

Dedication

The dedication is usually quite short, and is a personal rather than an academic recognition. The *Dedication* does not have to be titled, but it must appear in the table of contents. If you want to skip the chapter title but still enter it into the Table of Contents, use this command `\chapter[Dedication]{}`.

Note that this section is the last of the preliminary pages (with lowercase Roman numeral page numbers). It must be placed *before* the `\mainmatter` command. After that, Arabic numbered pages will begin.

Chapter 1

Background and Terminology

Chapter 2

Protecting Quantized CNNs against Rowhammer through Adversarial Training

Chapter 3

Measuring Fault Resilience of CNNs against Weight Faults

Chapter 4

Some Parameters are more Equal

4.1 Introduction

There are a variety of studies confirming that some parameters of deep neural networks (DNNs) play a more important role in the process of inference. These studies include but are not limited to DNN compression through weight pruning, saliency analysis of network parameters, and ranking most influential parameters for performing weight perturbation attacks. Yet, the criticality of parameters in sense of being vulnerable to bit flips in presence of range restriction techniques is not investigated. In this chapter we analyze the case of ResNet50 image classifier with and without range restriction protection applied.

4.2 Experimental Setup

In this experiment we used ResNet50 as an image classifier. We used observed ranges from 20% of training data set for clipper protection. First we sampled 1000 out of ImageNet validation images and then selected the 80 images causing most of the SDCs overall.

To report the retrieval measures (i.e. precision and recall) we reduce the search space to 4000 randomly selected parameters uniformly across all the network. Further we report values for a technique which is capable of protecting 10% of the parameters (i.e. 400 parameters). The reported values in the result graphs are for selection of these 400 parameters out of 4000 assisted with some injection trials. In each technique, first the parameters are ranked. Then the number of trials are performed to verify the top ranking parameters. This verification obtains some parameters that are critical for sure and some parameters that are non-critical for sure. The certain critical parameters are selected to be protected and the reset of the 400 parameter protection budget is filled with the rest of top-ranking parameters. This

way we will always have a resulting set of 400 parameters out of 4000 parameters. True-positive is number of critical parameters among these 400, false-positive is number of non-critical parameters among these 400, true-negative is the number of non-critical parameters kept out of these 400, and false-negative is the number of critical parameters kept out.

To calculate the heuristics the gradient value is calculated regarding the cross entropy loss with regard to the 80 images. In the graphs *value* means the value of the parameter and *grad* the gradient calculated for that parameter.

4.3 Results

Whereas ranking the parameters by the heuristic $value/|grad|$ seems promising both with and without applying clipper as a protection technique as demonstrated in Figure 5.1, it turns out to be a proxy to identify the parameters which are in the last layer. If we plot the same measures excluding the injections to the parameters of the last layer as demonstrated in Figure 5.2, we will see that $|grad|$ will be a better heuristic after applying clipper protection. Nevertheless, $value/|grad|$ remains dominant if we don't protect the network.

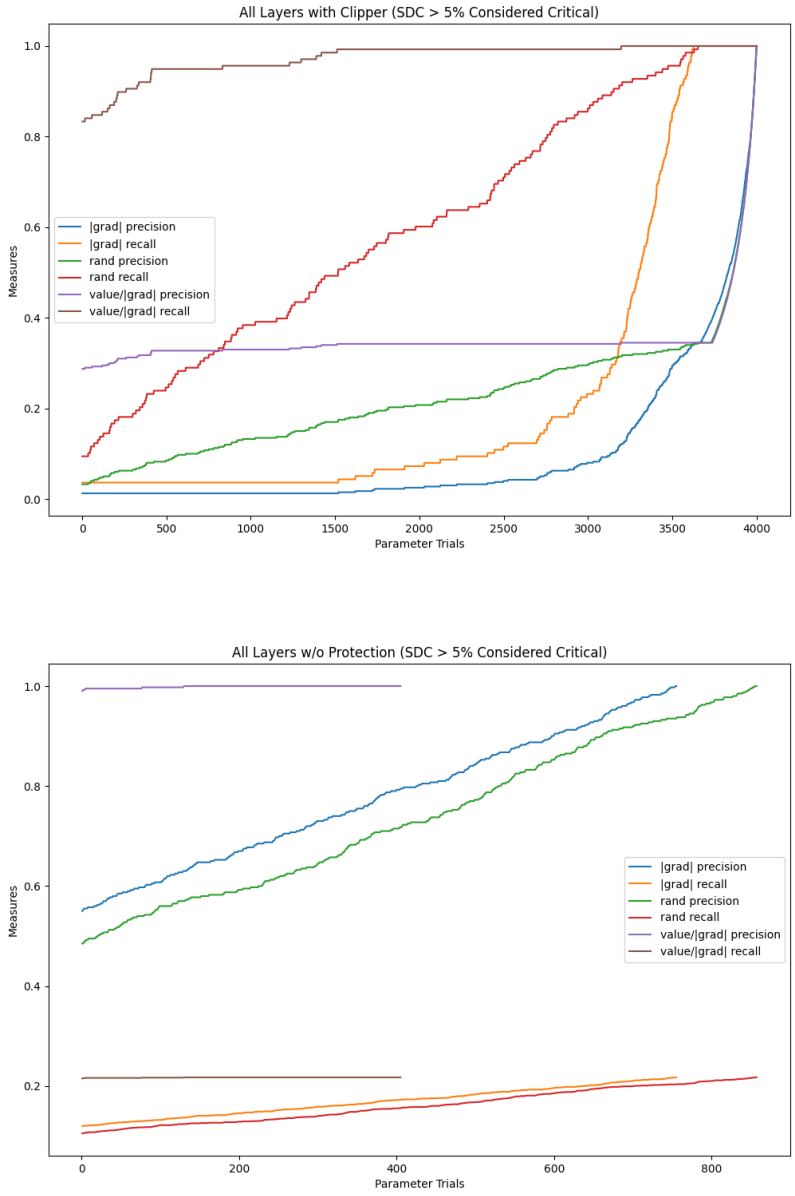

Figure 4.1: Performance of heuristics in comparison to random parameter selection. Including injections to all layers.

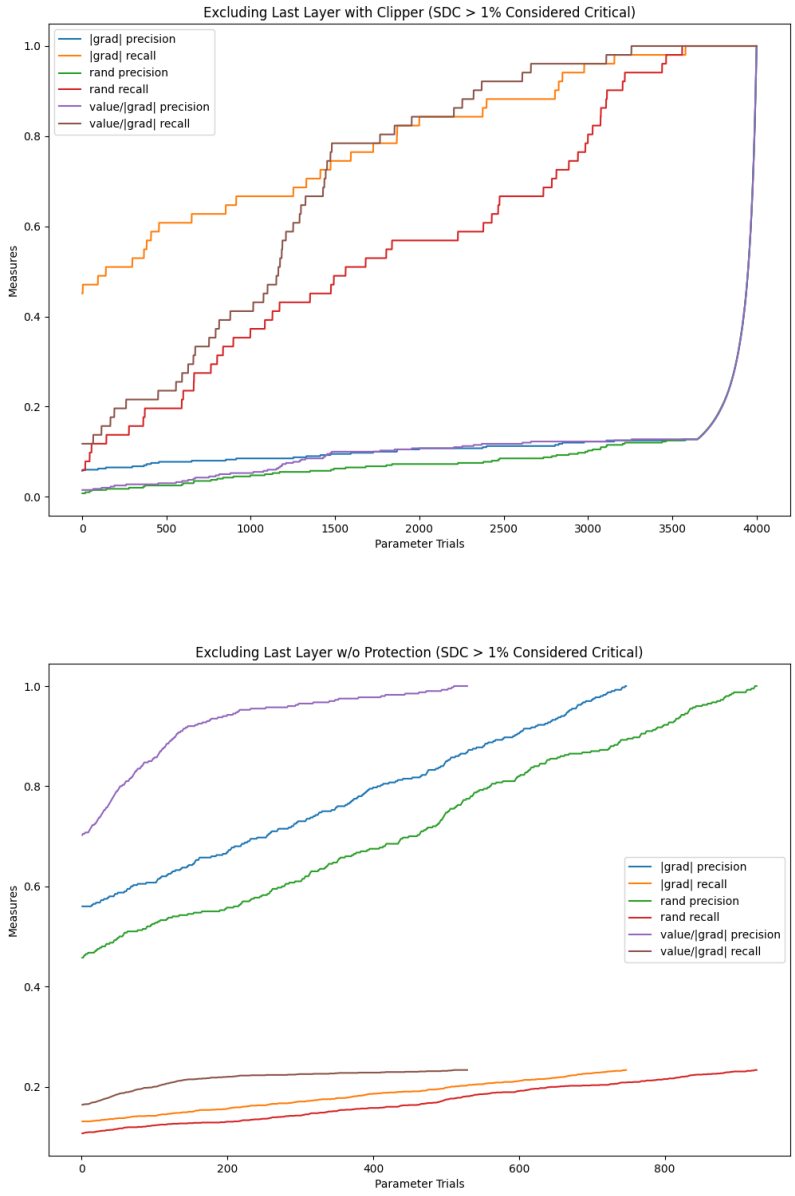

Figure 4.2: Performance of heuristics in comparison to random parameter selection. Excluding the injections to the last layer.

Chapter 5

This is a Chapter

5.1 A Section

Here is a section with some text. Equations look like this $y = x$.[1]

This is an example of a second paragraph in a section so you can see how much it is indented by.

5.1.1 This is a Subsection

Here is an example of a citation: [**?**]. The actual form of the citation is governed by the bibliographystyle. These citations are maintained in a BIBTeX file `sample.bib`. You could type these directly into the file. For an example of the format to use look at the file `ubcsample.bbl` after you compile this file.[2]

This is an example of a second paragraph in a subsection so you can see how much it is indented by.

This is a Subsubsection

Here are some more citations [**?** **?** **?**]. If you use the `natbib` package with the `sort&compress` option, then the following citation will look the same as the first citation in this section: [**?** **?** **?**].

This is an example of a second paragraph in a subsubsection so you can see how much it is indented by.

This is a Paragraph Paragraphs and subparagraphs are the smallest units of text. There is no subsubsubsection etc.

This is a Subparagraph This is the last level of organisation. If you need more than this, you should consider reorganizing your work...

[1] Here is a footnote.

[2] Here is another footnote.

Phoenix	$960.35
Calgary	$250.00

Table 5.1: Here is the caption for this wonderful table. It has not been centered and the positioning has been specified to be at the top of the page. Thus it appears above the babble rather than below where it is defined in the source file.

$$\mathrm{f}(x) = \int_{-\infty}^{\int_{-\infty}^{x} e^{-\frac{y^2}{2}}\,\mathrm{d}y} e^{-z^2}\,\mathrm{d}z \tag{5.1}$$

In order to show you what a separate page would look like (i.e. without a chapter heading) I must type some more text. Thus I will babble a bit and keep babbling for at least one more page. . . What you should notice is that the chapter titles appear substantially lower than the continuing text. Babble babble.

Babble babble.

5.2 Quote

Here is a quote:

> This is a small poem,
> a little poem, a Haiku,
> to show you how to.
> —Michael M^{c}Neil Forbes.

This small poem shows several features:

- The use of the `quote` and `center` environments.
- The `\newpage` command has been used to force a page break. (Sections do not usually start on a new page.)
- The pagestyle has been set to suppress the headers using the command `\thispagestyle{plain}`. Note that using `\pagestyle{plain}` would have affected all of the subsequent pages.

5.3 Programs

Here we give an example of a new float as defined using the `float` package. In the preamble we have used the commands

```
\floatstyle{ruled}
\newfloat{Program}{htbp}{lop}[chapter]
```

This creates a "Program" environment that may be used for program fragments. A sample `python` program is shown in Program 6.1. (Note that Python places a fairly restrictive limit on recursion so trying to call this with a large n before building up the cache is likely to fail unless you increase the recursion depth.) Instead of using a `verbatim` environment for your program chunks, you might like to `include` them within an `alltt` envrironment by including the `\usepackage{alltt}` package (see page 187 of the LaTeX book). Another useful package is the `\usepackage{listings}` which can pretty-print many different types of source code.

Program 5.1 Python program that computes the n^{th} Fibonacci number using memoization.

```
def fib(n,_cache={}):
    if n < 2:
        return 1
    if n in _cache:
        return _cache[n]
    else:
        result = fib(n-1)+fib(n-2)
        _cache[n] = result
        return result
```

Chapter 6

Another Chapter with a Very Long Chapter-name that will Probably Cause Problems

This chapter name is very long and does not display properly in the running headers or in the table of contents. To deal with this, we provide a shorter version of the title as the optional argument to the `\chapter[]{}` command.

For example, this chapter's title and associated table of contents heading and running header was created with
`\chapter[Another Chapter\ldots]{Another Chapter with a Very Long Chapter-name that will Probably Cause Problems}`.

Note that, according to the thesis regulations, the heading included in the table of contents must be a truncation of the actual heading.

This Chapter was used as a demonstration in the Preface for how to attribute contribution from collaborators. If there are any such contributions, details must be included in the Preface. If you wish, you may additionally use a footnote such as this.[3]

6.1 Another Section

Another bunch of text to demonstrate what this file does. You might want a list for example:[4]

- An item in a list.
- Another item in a list.

[3] This chapter is based on work conducted in UBC's Maple Syrup Laboratory by Dr. A. Apple, Professor B. Boat, and C. Cat.

[4] Here is a footnote in a different chapter. Footnotes should come after punctuation.

An Unnumbered Section That is Not Included in the Table of Contents

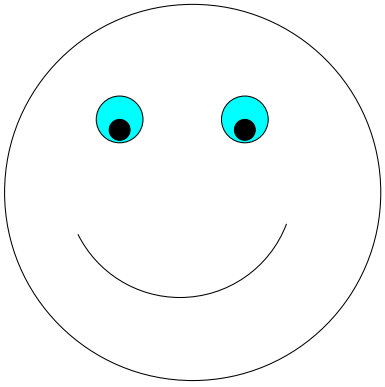

Figure 6.1: This is a figure of a happy face with a `psfrag` replacement. The original figure (drawn in xfig and exported to a .eps file) has the text "pie makes me happy!". The `psfrag` package replaces this with "π makes me happy!". Note: the Makefile compiles the sample using pdfLaTeX which cannot use `psfrag` directly. For some options that work with pdfLaTeX, please see this discussion: `http://tex.stackexchange.com/questions/11839`. For the caption, we have used the optional argument for the caption command so that only a short version of this caption occurs in the list of figures.

Here is an example of a figure environment. Perhaps I should say that the example of a figure can be seen in Figure 7.1. Figure placement can be tricky with LaTeX because figures and tables are treated as "floats": text can flow around them, but if there is not enough space, they will appear later. To prevent figures from going too far, the `\afterpage{\clearpage}` command can be used. This makes sure that the figure are typeset at the end of the page (possibly appear on their own on the following pages) and before any subsequent text.

The `\clearpage` forces a page break so that the figure can be placed, but without the the `\afterpage{}` command, the page would be broken too early (at the `\clearpage` statement). The `\afterpage{}` command

tells LaTeX to issue the command after the present page has been rendered.

6.2 Tables

We have already included one table: 6.1. Another table is plopped right here. Well, actually, as with Figures, tables do not necessarily appear right

	Singular		Plural	
	English	**Gaeilge**	English	**Gaeilge**
1st Person	at me	**agam**	at us	**againn**
2nd Person	at you	**agat**	at you	**agaibh**
3rd Person	at him	**aige**	at them	**acu**
	at her	**aici**		

Table 6.1: Another table.

"here" because tables are also "floats". LaTeX puts them where it can. Because of this, one should refer to floats by their labels rather than by their location. This example is demonstrated by Table 7.1. This one is pretty close, however. (Note: you should generally not put tables or figures in the middle of a paragraph. This example is for demonstration purposes only.)

Another useful package is `\usepackage{longtable}` which provides the `longtable` environment. This is nice because it allows tables to span multiple pages. Table 7.2 has been formatted this way.

Table 6.2: Feasible triples for highly variable Grid

Time (s)	**Triple chosen**	**Other feasible triples**
0	(1, 11, 13725)	(1, 12, 10980), (1, 13, 8235), (2, 2, 0), (3, 1, 0)
274	(1, 12, 10980)	(1, 13, 8235), (2, 2, 0), (2, 3, 0), (3, 1, 0)
5490	(1, 12, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
8235	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
10980	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
13725	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
16470	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
19215	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
21960	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)

Continued on next page

Table 6.2 – continued from previous page

Time (s)	Triple chosen	Other feasible triples
24705	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
27450	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
30195	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
32940	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
35685	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
38430	(1, 13, 10980)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
41175	(1, 12, 13725)	(1, 13, 10980), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
43920	(1, 13, 10980)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
46665	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
49410	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
52155	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
54900	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
57645	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
60390	(1, 12, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
63135	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
65880	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
68625	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
71370	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
74115	(1, 12, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
76860	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
79605	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
82350	(1, 12, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
85095	(1, 12, 13725)	(1, 13, 10980), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
87840	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
90585	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
93330	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
96075	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
98820	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
101565	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
104310	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
107055	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
109800	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
112545	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
115290	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
118035	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
120780	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)

Continued on next page

Table 6.2 – continued from previous page

Time (s)	Triple chosen	Other feasible triples
123525	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
126270	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
129015	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
131760	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
134505	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
137250	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
139995	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
142740	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
145485	(1, 12, 16470)	(1, 13, 13725), (2, 2, 2745), (2, 3, 0), (3, 1, 0)
148230	(2, 2, 2745)	(2, 3, 0), (3, 1, 0)
150975	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
153720	(1, 12, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
156465	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
159210	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
161955	(1, 13, 16470)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)
164700	(1, 13, 13725)	(2, 2, 2745), (2, 3, 0), (3, 1, 0)

An Unnumbered Subsection

Note that if you use subsections or further divisions under an unnumbered section, then you should make them unnumbered as well otherwise you will end up with zeros in the section numbering.

Chapter 7

Landscape Mode

The landscape mode allows you to rotate a page through 90 degrees. It is generally not a good idea to make the chapter heading landscape, but it can be useful for long tables etc.

This text should appear rotated, allowing for formatting of very wide tables etc. Note that this might only work after you convert the `dvi` file to a postscript (`ps`) or `pdf` file using `dvips` or `dvipdf` etc. This feature is provided by the `lscape` and the `pdflscape` packages. The latter is preferred if it works as it also rotates the pages in the pdf file for easier viewing.

Appendix A

First Appendix

Here you can have your appendices. Note that if you only have a single appendix, you should issue `\renewcommand{\appendicesname}{Appendix}` before calling `\appendix` to display the singular "Appendix" rather than the default plural "Appendices".

Appendix B

Second Appendix

Here is the second appendix.

Additional Information

This chapter shows you how to include additional information in your thesis, the removal of which will not affect the submission. Such material should be removed before the thesis is actually submitted.

First, the chapter is unnumbered and not included in the Table of Contents. Second, it is the last section of the thesis, so its removal will not alter any of the page numbering etc. for the previous sections. Do not include any floats, however, as these will appear in the initial lists.

The `ubcthesis` LaTeX class has been designed to aid you in producing a thesis that conforms to the requirements of The University of British Columbia Faculty of Graduate Studies (FoGS).

Proper use of this class and sample is highly recommended—and should produce a well formatted document that meets the FoGS requirement. Notwithstanding, complex theses may require additional formatting that may conflict with some of the requirements. We therefore *highly recommend* that you consult one of the FoGS staff for assistance and an assessment of potential problems *before* starting final draft.

While we have attemped to address most of the thesis formatting requirements in these files, they do not constitute an official set of thesis requirements. The official requirements are available at the following section of the FoGS web site:

`http://www.grad.ubc.ca/current-students/dissertation-thesis-preparation`

We recommend that you review these instructions carefully.