






1 Isabelle/Solidity for Smart Contracts

2 Jane Open Access   

3 Dummy University Computing Laboratory, [optional: Address], Country

4 My second affiliation, Country

5 Joan R. Public¹  

6 Department of Informatics, Dummy College, [optional: Address], Country

7 — Abstract —

8 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent convallis orci arcu, eu mollis dolor.
9 Aliquam eleifend suscipit lacinia. Maecenas quam mi, porta ut lacinia sed, convallis ac dui. Lorem
10 ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.

11 **2012 ACM Subject Classification** Replace `ccsdsc` macro with valid one

12 **Keywords and phrases** Program Verification, Smart Contracts, Isabelle, Solidity

13 **Digital Object Identifier** 10.4230/OASICS.CVIT.2016.23

14 **Funding** Jane Open Access: (Optional) author-specific funding acknowledgements

15 Joan R. Public: [funding]

16 **Acknowledgements** I want to thank ...

17 1 Introduction

18 OASICS is a series of open access high-quality conference proceedings across all fields in
19 informatics established in cooperation with Schloss Dagstuhl. In order to do justice to the
20 high scientific quality of the conferences that publish their proceedings in the OASICS series,
21 which is ensured by the thorough review process of the respective events, we believe that
22 OASICS proceedings must have an attractive and consistent layout matching the standard
23 of the series. Moreover, the quality of the metadata, the typesetting and the layout must
24 also meet the requirements of other external parties such as indexing service, DOI registry,
25 funding agencies, among others. The guidelines contained in this document serve as the
26 baseline for the authors, editors, and the publisher to create documents that meet as many
27 different requirements as possible.

28 Please comply with the following instructions when preparing your article for a OASICS
29 proceedings volume.

30 Minimum requirements

- 31 ■ Use pdf_latex and an up-to-date L^AT_EX system.
- 32 ■ Use further L^AT_EX packages and custom made macros carefully and only if required.
- 33 ■ Use the provided sectioning macros: `\section`, `\subsection`, `\subsubsection`,
34 `\paragraph`, `\paragraph*`, and `\subparagraph*`.
- 35 ■ Provide suitable graphics of at least 300dpi (preferably in PDF format).
- 36 ■ Use BibT_EX and keep the standard style (`plainurl`) for the bibliography.
- 37 ■ Please try to keep the warnings log as small as possible. Avoid overfull `\hboxes` and any
38 kind of warnings/errors with the referenced BibT_EX entries.
- 39 ■ Use a spellchecker to correct typos.

¹ Optional footnote, e.g. to mark corresponding author



40 **Mandatory metadata macros**

41 Please set the values of the metadata macros carefully since the information parsed from
 42 these macros will be passed to publication servers, catalogues and search engines. Avoid
 43 placing macros inside the metadata macros. The following metadata macros/environments
 44 are mandatory:

- 45 ■ `\title` and, in case of long titles, `\titlerunning`.
- 46 ■ `\author`, one for each author, even if two or more authors have the same affiliation.
- 47 ■ `\authorrunning` and `\Copyright` (concatenated author names)
 48 The `\author` macros and the `\Copyright` macro should contain full author names (espe-
 49 cially with regard to the first name), while `\authorrunning` should contain abbreviated
 50 first names.
- 51 ■ `\ccsdesc` (ACM classification, see <https://www.acm.org/publications/class-2012>).
- 52 ■ `\keywords` (a comma-separated list of keywords).
- 53 ■ `\relatedversion` (if there is a related version, typically the “full version”); please make
 54 sure to provide a persistent URL, e.g., at arXiv.
- 55 ■ `\begin{abstract}... \end{abstract}` .

56 **Please do not ...**

57 Generally speaking, please do not override the `oasics-v2021`-style defaults. To be more
 58 specific, a short checklist also used by Dagstuhl Publishing during the final typesetting is
 59 given below. In case of **non-compliance** with these rules Dagstuhl Publishing will remove
 60 the corresponding parts of L^AT_EX code and **replace it with the `oasics-v2021` defaults**.
 61 In serious cases, we may reject the L^AT_EX-source and expect the corresponding author to
 62 revise the relevant parts.

- 63 ■ Do not use a different main font. (For example, the `times` package is forbidden.)
- 64 ■ Do not alter the spacing of the `oasics-v2021.cls` style file.
- 65 ■ Do not use `enumitem` and `paralist`. (The `enumerate` package is preloaded, so you can
 66 use `\begin{enumerate}[(a)]` or the like.)
- 67 ■ Do not use “self-made” sectioning commands (e.g., `\noindent{\bf My Paragraph}`).
- 68 ■ Do not hide large text blocks using comments or `\iffalse ... \fi` constructions.
- 69 ■ Do not use conditional structures to include/exclude content. Instead, please provide
 70 only the content that should be published – in one file – and nothing else.
- 71 ■ Do not wrap figures and tables with text. In particular, the package `wrapfig` is not
 72 supported.
- 73 ■ Do not change the bibliography style. In particular, do not use author-year citations.
 74 (The `natbib` package is not supported.)

75 This is only a summary containing the most relevant details. Please read the complete
 76 document “OASICS: Instructions for Authors and the `oasics-v2021` Class” for all details
 77 and don’t hesitate to contact Dagstuhl Publishing (<mailto:publishing@dagstuhl.de>) in
 78 case of questions or comments: [http://drops.dagstuhl.de/styles/oasics-v2021/](http://drops.dagstuhl.de/styles/oasics-v2021/oasics-v2021-authors/oasics-v2021-authors-guidelines.pdf)
 79 [oasics-v2021-authors/oasics-v2021-authors-guidelines.pdf](http://drops.dagstuhl.de/styles/oasics-v2021/oasics-v2021-authors/oasics-v2021-authors-guidelines.pdf)

80 **2 Overview**

81 Lorem ipsum dolor sit amet, consectetur adipiscing elit [4]. Praesent convallis orci arcu, eu
 82 mollis dolor. Aliquam eleifend suscipit lacinia. Maecenas quam mi, porta ut lacinia sed,
 83 convallis ac dui. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.
 84 Donec eget odio et magna ullamcorper vehicula ut vitae libero. Maecenas lectus nulla, auctor

■ **Listing 1** Useless code.

```
for i:=maxint to 0 do
begin
  j:=square(root(i));
end;
```

85 nec varius ac, ultricies et turpis. Pellentesque id ante erat. In hac habitasse platea dictumst.
 86 Curabitur a scelerisque odio. Pellentesque elit risus, posuere quis elementum at, pellentesque
 87 ut diam. Quisque aliquam libero id mi imperdiet quis convallis turpis eleifend.

88 ► **Lemma 1** (Lorem ipsum). *Vestibulum sodales dolor et dui cursus iaculis. Nullam ullam-*
 89 *corper purus vel turpis lobortis eu tempus lorem semper. Proin facilisis gravida rutrum.*
 90 *Etiam sed sollicitudin lorem. Proin pellentesque risus at elit hendrerit pharetra. Integer at*
 91 *turpis varius libero rhoncus fermentum vitae vitae metus.*

92 **Proof.** Cras purus lorem, pulvinar et fermentum sagittis, suscipit quis magna.

93 **Just some paragraph within the proof.** Nam liber tempor cum soluta nobis eleifend option
 94 congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum
 95 dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut
 96 laoreet dolore magna aliquam erat volutpat.

97 ▷ **Claim 2.** content...

98 Proof. content...

99 1. abc abc abc

100

101 ► **Corollary 3** (Curabitur pulvinar, [2]). *Nam liber tempor cum soluta nobis eleifend option*
 102 *congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum*
 103 *dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut*
 104 *laoreet dolore magna aliquam erat volutpat.*

105 ► **Proposition 4.** *This is a proposition*

106 Proposition 4 and Proposition 4 . . .

107 2.1 Curabitur dictum felis id sapien

108 Curabitur dictum Corollary 3 felis id sapien Corollary 3 mollis ut venenatis tortor feugiat.
 109 Curabitur sed velit diam. Integer aliquam, nunc ac egestas lacinia, nibh est vehicula nibh, ac
 110 auctor velit tellus non arcu. Vestibulum lacinia ipsum vitae nisi ultrices eget gravida turpis
 111 laoreet. Duis rutrum dapibus ornare. Nulla vehicula vulputate iaculis. Proin a consequat
 112 neque. Donec ut rutrum urna. Morbi scelerisque turpis sed elit sagittis eu scelerisque quam
 113 condimentum. Pellentesque habitant morbi tristique senectus et netus et malesuada fames
 114 ac turpis egestas. Aenean nec faucibus leo. Cras ut nisl odio, non tincidunt lorem. Integer
 115 purus ligula, venenatis et convallis lacinia, scelerisque at erat. Fusce risus libero, convallis at
 116 fermentum in, dignissim sed sem. Ut dapibus orci vitae nisl viverra nec adipiscing tortor
 117 condimentum [1]. Donec non suscipit lorem. Nam sit amet enim vitae nisl accumsan pretium.

118 **2.2 Proin ac fermentum augue**

119 Proin ac fermentum augue. Nullam bibendum enim sollicitudin tellus egestas lacinia euismod
 120 orci mollis. Nulla facilisi. Vivamus volutpat venenatis sapien, vitae feugiat arcu fringilla ac.
 121 Mauris sapien tortor, sagittis eget auctor at, vulputate pharetra magna. Sed congue, dui
 122 nec vulputate convallis, sem nunc adipiscing dui, vel venenatis mauris sem in dui. Praesent
 123 a pretium quam. Mauris non mauris sit amet eros rutrum aliquam id ut sapien. Nulla
 124 aliquet fringilla sagittis. Pellentesque eu metus posuere nunc tincidunt dignissim in tempor
 125 dolor. Nulla cursus aliquet enim. Cras sapien risus, accumsan eu cursus ut, commodo vel
 126 velit. Praesent aliquet consectetur ligula, vitae iaculis ligula interdum vel. Integer faucibus
 127 faucibus felis.

- 128 ■ Ut vitae diam augue.
- 129 ■ Integer lacus ante, pellentesque sed sollicitudin et, pulvinar adipiscing sem.
- 130 ■ Maecenas facilisis, leo quis tincidunt egestas, magna ipsum condimentum orci, vitae
 131 facilisis nibh turpis et elit.

132 ► Remark 5. content...

133 **3 Case Study**

134 Nec urna malesuada sollicitudin. Nulla facilisi. Vivamus aliquam tempus ligula eget ornare.
 135 Praesent eget magna ut turpis mattis cursus. Aliquam vel condimentum orci. Nunc congue,
 136 libero in gravida convallis [3], orci nibh sodales quam, id egestas felis mi nec nisi. Suspendisse
 137 tincidunt, est ac vestibulum posuere, justo odio bibendum urna, rutrum bibendum dolor sem
 138 nec tellus.

139 ► **Lemma 6** (Quisque blandit tempus nunc). *Sed interdum nisl pretium non. Mauris sodales
 140 consequat risus vel consectetur. Aliquam erat volutpat. Nunc sed sapien ligula. Proin faucibus
 141 sapien luctus nisl feugiat convallis faucibus elit cursus. Nunc vestibulum nunc ac massa
 142 pretium pharetra. Nulla facilisis turpis id augue venenatis blandit. Cum sociis natoque
 143 penatibus et magnis dis parturient montes, nascetur ridiculus mus.*

144 Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui. Nam
 145 vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa sit
 146 amet neque.

147 **4 Specification**

148 Morbi eros magna, vestibulum non posuere non, porta eu quam. Maecenas vitae orci risus,
 149 eget imperdiet mauris. Donec massa mauris, pellentesque vel lobortis eu, molestie ac turpis.
 150 Sed condimentum convallis dolor, a dignissim est ultrices eu. Donec consectetur volutpat
 151 eros, et ornare dui ultricies id. Vivamus eu augue eget dolor euismod ultrices et sit amet nisi.
 152 Vivamus malesuada leo ac leo ullamcorper tempor. Donec justo mi, tempor vitae aliquet non,
 153 faucibus eu lacus. Donec dictum gravida neque, non porta turpis imperdiet eget. Curabitur
 154 quis euismod ligula.

155 **References**

- 156 1 Edsger W. Dijkstra. Letters to the editor: go to statement considered harmful. *Commun.*
 157 *ACM*, 11(3):147–148, 1968. doi:10.1145/362929.362947.

- 158 2 Jim Gray and Andreas Reuter. *Transaction Processing: Concepts and Techniques*. Morgan
 159 Kaufmann, 1993.
- 160 3 John E. Hopcroft, Wolfgang J. Paul, and Leslie G. Valiant. On time versus space and
 161 related problems. In *16th Annual Symposium on Foundations of Computer Science, Berkeley,
 162 California, USA, October 13-15, 1975*, pages 57–64. IEEE Computer Society, 1975. doi:
 163 10.1109/SFCS.1975.23.
- 164 4 Donald E. Knuth. Computer Programming as an Art. *Commun. ACM*, 17(12):667–673, 1974.
 165 doi:10.1145/361604.361612.

166 A Styles of lists, enumerations, and descriptions

167 List of different predefined enumeration styles:

- 168 ■ `\begin{itemize}...\end{itemize}`
 169 ■ ...
 170 ■ ...
- 171 1. `\begin{enumerate}...\end{enumerate}`
 172 2. ...
 173 3. ...
- 174 (a) `\begin{alphaenumerate}...\end{alphaenumerate}`
 175 (b) ...
 176 (c) ...
- 177 (i) `\begin{romanenumerate}...\end{romanenumerate}`
 178 (ii) ...
 179 (iii) ...
- 180 (1) `\begin{bracketenumerate}...\end{bracketenumerate}`
 181 (2) ...
 182 (3) ...
- 183 **Description 1** `\begin{description} \item[Description 1] ... \end{description}`
 184 **Description 2** Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.
 185 Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus
 186 massa sit amet neque.
- 187 **Description 3** ...
- 188 Proposition 10 and Proposition 10 ...

189 B Theorem-like environments

190 List of different predefined enumeration styles:

- 191 ► **Theorem 7.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 192 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 193 *sit amet neque.*
- 194 ► **Lemma 8.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 195 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 196 *sit amet neque.*

197 ► **Corollary 9.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 198 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 199 *sit amet neque.*

200 ► **Proposition 10.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo*
 201 *dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 202 *massa sit amet neque.*

203 ► **Conjecture 11.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo*
 204 *dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 205 *massa sit amet neque.*

206 ► **Observation 12.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et*
 207 *leo dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 208 *massa sit amet neque.*

209 ► **Exercise 13.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo*
 210 *dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 211 *massa sit amet neque.*

212 ► **Definition 14.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo*
 213 *dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 214 *massa sit amet neque.*

215 ► **Example 15.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo*
 216 *dui. Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus*
 217 *massa sit amet neque.*

218 ► **Note 16.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 219 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 220 *sit amet neque.*

221 ► **Note.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui. Nam*
 222 *vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa sit*
 223 *amet neque.*

224 ► **Remark 17.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 225 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 226 *sit amet neque.*

227 ► **Remark.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 228 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 229 *sit amet neque.*

230 ▷ **Claim 18.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 231 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 232 *sit amet neque.*

233 ▷ **Claim.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui.*
 234 *Nam vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa*
 235 *sit amet neque.*

236 ► **Proof.** *Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui. Nam*
 237 *vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa sit*
 238 *amet neque.* ◀

239 Proof. Fusce eu leo nisi. Cras eget orci neque, eleifend dapibus felis. Duis et leo dui. Nam
240 vulputate, velit et laoreet porttitor, quam arcu facilisis dui, sed malesuada risus massa sit
241 amet neque. 