

# The `tugPoster` Package

Markus Quaritsch

April 12, 2018

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Creating a Poster</b>	<b>2</b>
2.1	Minimal Working Example . . . . .	2
2.2	Adjusting Poster Size . . . . .	3
2.3	Author, Affiliation, Email Addresses . . . . .	3
2.4	Footer . . . . .	3
2.4.1	Advanced Footer Layout . . . . .	5
2.5	Main Content . . . . .	5
2.5.1	Subheader, Subsubheader . . . . .	7
2.6	Bullet Lists . . . . .	8
2.7	Figures . . . . .	8
2.8	Abstract . . . . .	9
2.9	References . . . . .	10
2.10	Advanced Layouts . . . . .	10
2.10.1	Relative Lengths . . . . .	10
2.10.2	Three Column Content . . . . .	11
2.10.3	Custom Institute Banner . . . . .	12
2.10.4	Customizing Colors . . . . .	12
2.11	Preparing for Print . . . . .	12
<b>3</b>	<b>Summary of Commands/Environments/Options</b>	<b>13</b>
<b>4</b>	<b>Examples</b>	<b>15</b>
<b>5</b>	<b>Debugging / Layout Support</b>	<b>15</b>
<b>6</b>	<b>Known Issues</b>	<b>15</b>

# 1 Introduction

The intention of this  $\text{\LaTeX}$  class is on the one hand to greatly simplify the process of creating posters and on the other hand to produce nice-looking posters that follow the TU Graz design guidelines. The `tugPoster` class makes among others heavy use of the  $\text{\LaTeX}$  packages `tcolorbox`, `tikz` and `enumitem`.

This document describes the options, commands, and environments defined within the `tugPoster` class and how you can use them to create a poster. All commands defined by `tugPoster` use the prefix `IPT`.

## 2 Creating a Poster

### 2.1 Minimal Working Example

To start with creating a new poster we use the following code:

**Listing 1: Minimal Working Example**

```
1 \documentclass{tugPoster}

3 % set path where all required images can be found
4 \graphicspath{{../../img/}}

6 % configure name, address and contact info of the
  institute
7 \IPTInstituteName{Institute of \LaTeX{} Experts}
8 \IPTInstituteAddress{Rechbauerstraße 12, 8010
  Graz, Austria}
9 \IPTInstituteURL{latex.tugraz.at}
10 \IPTInstituteEmail{noreply@tugraz.at}
11 \IPTInstituteShort{Short}

13 % set title of the poster
14 \title{Poster Title}

16 % start with the poster...
17 \begin{document}
18   \maketitle
19 \end{document}
```



The  $\text{\LaTeX}$  code in Listing 1 should produce a PDF document of size A0 (841 mm  $\times$  1189 mm) with the main layout elements (i.e., the institute's short name on the left, the TU Graz logo and claim on top and the institute name and address, etc.)

## 2.2 Adjusting Poster Size

The `tugPoster` package supports different paper sizes for the poster. To select a certain size simply add the option `size=` followed by a supported poster size to the document class options. The supported poster sizes are listed in Section 3

### Listing 1: Adding authors

```
[...]  
1 | \documentclass[size=A1]{tugPoster}  
[...]
```



## 2.3 Author, Affiliation, Email Addresses

The authors can be typeset either in one column or if necessary in two columns. Therefore, the commands `\authorName<A/B>`, `\authorAffiliation<A/B>`, and `\authorEmail<A/B>` can be used. Contents of the commands with the suffix A are put on the left column while the others are placed on the right column. If only the commands with suffix A are used then the authors can span the whole page width (see Listing 2).

### Listing 2: Adding authors

```
[...]  
14 | \title{Poster Title}  
  
16 | \authorNameA{Author Name, Author Name, Author  
17 |     Name, Author Name, Author Name, Author Name}  
17 | \authorAffiliationA{Institute for \LaTeX{}  
18 |     Experts, Graz University of Technology}  
18 | \authorEmailA{Email@Address}  
  
20 | \begin{document}  
[...]
```



## 2.4 Footer

In the footer there is some space reserved for partner and/or sponsor logos. In addition there is a QR-code that points to a landing-page on the institute's website.

By default the QR-code points to the institute's website. In case the QR-code shall point to a landing page or a more specific sub-page (e.g., project page), you can

add this as optional first argument to `\IPTInstituteUrl`. Please make sure to use the correct URL and that the QR-code points to the correct web page (cf. Listing 3). The QR-code can also be omitted using the statement `\NoQRCode` (cf: Listing 4). You can also place an NFC tag behind the poster with some additional information or data. This can be indicated by an according logo using the statement `\ShowNFC` (cf. Listing 5).

### **Listing 3: Adapting QR-Code target URL**

```
[...]
8 \IPTInstituteAddress{Rechbauerstraße 12, 8010
9   Graz, Austria}
10 \IPTInstituteURL[https://latex.tugraz.at/vorlagen
11   /allgemein]{latex.tugraz.at}
12 \IPTInstituteEmail{noreply@tugraz.at}
13 [...]
```



### **Listing 4: Omitting the QR-Code**

```
[...]
9 \IPTInstituteURL{latex.tugraz.at}
10 \NoQRCode
11 \IPTInstituteEmail{noreply@tugraz.at}
12 [...]
```



### **Listing 5: Showing the NFC icon**

```
[...]
9 \IPTInstituteURL[https://latex.tugraz.at/vorlagen
10   /allgemein]{latex.tugraz.at}
11 \ShowNFC
12 \IPTInstituteEmail{noreply@tugraz.at}
13 [...]
```



For adding partner and/or sponsor logos to the footer, the command `\IPTpartner` is provided. Using this command an arbitrary number of partner-logos can be added in the footer. This command has to come before `\begin{document}`. The logos are vertically aligned and horizontally distributed and limited to a maximum height. If you need to adjust individual logos (e.g., make it smaller), you can provide the optional

argument `imgoptions:]` which contains options for the the `\includegraphics` command.

An additional note can be placed at the top of the footer with the `\IPTpartnersNote` command.

#### Listing 6: Partner logos in the footer

```
[...]
20 \IPTpartnersNote{This project is sponsored by \
    .dots}
21 \IPTpartner{partner1}
22 \IPTpartner{partner2}

24 \begin{document}
[...]
```



#### 2.4.1 Advanced Footer Layout

In case you want to add further content or have special placement constraints an alternative command `\IPTpartners` is provided. The argument given to this command is placed in a minipage so you can add arbitrary contents.

Listing 7 shows an example how a number of images with different height can be vertically aligned to the center (note: for demonstration purpose a simple `\framebox` is used in the example. You can replace this with an `\includegraphics` command). In addition a single line of text can be added to the footer using the command `\IPTpartnersNote` mentioning funding contracts etc.

#### Listing 7: Custom footer layout

```
[...]
20 \IPTpartners{
21     \centering
22     \raisebox{-75pt}{\framebox(700,150){}}
23     \hspace*{180mm}
24     \raisebox{-50pt}{\framebox(400,100){}}
25 }

27 \begin{document}
[...]
```



### 2.5 Main Content

The main content is composed of several content blocks. Every content block has a title and some content. The title is set in a blue large bold font and has a rule below indicating the width of the content block.

The content blocks can either span the whole page width or can be placed in the left or right columns. It is not necessary that the whole poster is either single column or two columns. This can be mixed as necessary and as the content allows.

A basic content block is added by using the environment `IPTblock` (see Listing 8). The mandatory argument is the title of the content block. By default, the content block spans the whole page width and the content inside the content block is typeset in a single column.

#### **Listing 8: Basic Content Block**

```
[...]
27 \begin{document}
28   \maketitle
29
30   \begin{IPTblock}{Block Header}
31     Lorem ipsum dolor sit amet \ldots
32   \end{IPTblock}
33 \end{document}
[...]
```



If you want to place two content blocks next to each other (i.e., use a two-column layout) you have to use the environment `IPTtwocol` (see Listing 9). Inside the environment is the content for the left column, followed by the command `\IPTcolbreak` and then the content for the right column. The content for both columns is usually a `IPTblock` content block. Of course, you can have more than one `IPTblock` in every column.

#### **Listing 9: Two-column layout**

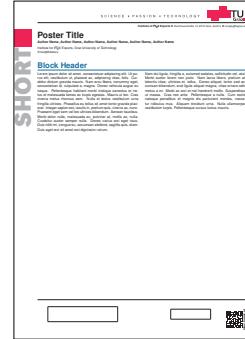
```
[...]
32 \begin{IPTtwocol}
33
34   \begin{IPTblock}{Block Header}
35     \lipsum[1]
36   \end{IPTblock}
37
38   \IPTcolbreak
39
40   \begin{IPTblock}{Block Header}
41     \lipsum[2]
42   \end{IPTblock}
43
44 \end{IPTtwocol}
[...]
```



The content within a content block can either be a single column or two columns. The easy way to typeset the content in two columns is to simply add the option `twocol` to the `IPTblock` environment (see Listing 10)

### Listing 10: Content block with two columns

```
[...]
32   \begin{IPTblock}[twocol]{Block Header}
33     \lipsum[1]
34   \IPTcolbreak
35     \lipsum[2]
36   \end{IPTblock}
[...]
```



Another way to typeset the content within a content block in two columns is to use the `IPTcols` environment. This environment produces a smaller gap between columns and should therefore **not** be used to separate columns at the first level but either to further split the content of the left or right column. On the top-level you can use `IPTtwocol` within a content block spanning the whole page width. `IPTcols` is more flexible concerning the subdivision of the columns. As mandatory argument you have to specify the width of the left column (between 0.0 and 1.0). This allows to have an image next to some text and use more space for the image or the text, depending on the situation. Obviously, after the `IPTcols` environment you can place further content which spans both columns (see Listing 11).

### Listing 11: Nested two-column layout

```
[...]
32   \begin{IPTblock}[twocol]{Block Header}
33     \begin{IPTcols}{0.5}
34       \lipsum[1]
35     \IPTcolbreak
36       \lipsum[2]
37     \end{IPTcols}
38   \IPTcolbreak
39     \lipsum[3-4]
40   \end{IPTblock}
[...]
```



For more complex layouts it is often the case that you need to place a figure next to some text and another figure below spans both columns, etc. In such cases it is necessary (and intended) to arbitrarily nest the above described environments `IPTblock`, `IPTtwocol`, and `IPTcols`.

#### 2.5.1 Subheader, Subsubheader

Within the content blocks you can add further headlines, i.e., subheader and subsubheader. Therefore, dedicated commands are available: `\IPTsection` and `\IPTsubsection` (see Listing 12).

### Listing 12: Subheader, Subsubheader

```
[...]
32   \begin{IPTblock}[twocol]{Section Headline}
33     \IPTsection{Subheader}
34     \lipsum[1]
35   \IPTcolbreak
36     \IPTsection{Subheader}
37     \lipsum[2]
38     \IPTsubsection{SubSubHeader}
39     \lipsum[4]
40   \end{IPTblock}
41 [...]
```



## 2.6 Bullet Lists

Bullet lists can be used as in every  $\text{\LaTeX}$  document via the `itemize` environment. Via the `enumitem` package the layout of the lists has been adapted to match the intended style. Up to three itemized lists can be nested (see Listing 13).

### Listing 13: Bullet Lists

```
[...]
32   \begin{IPTtwocol}
33     \begin{IPTblock}{Block Header}
34       \begin{itemize}
35         \item Item 1
36         \item Item 2
37           \begin{itemize}
38             \item Item 2.1
39               \begin{itemize}
40                 \item Item 2.1.1
41               \end{itemize}
42             \end{itemize}
43           \end{itemize}
44         \end{IPTblock}
45       \end{IPTtwocol}
46 [...]
```



## 2.7 Figures

Adding figures to a latex document and placing them at a certain position is always cumbersome in  $\text{\LaTeX}$  documents. Hence, we provide a new command `\IPTgraphics` that allows to easily add figures at a certain position. `\IPTgraphics` takes an optional

argument with of key-value options as described below and a mandatory argument of the file name to include.

`IPTgraphics` supports the following arguments:

`imgoptions`: this is a list of options that is directly passed to the `\includegraphics` command. here you can adjust the size of the image, rotate or crop the image, etc.

`caption`: here you can specify the caption which is typeset below the image

`label`: allows to define a label for the figure that can be used in a `\ref` command

The content block added via `IPTgraphics` always spans the current maximum text width/column width. If you want to use more or less space for the image you need to adjust the text width (i.e. the column width). As option for the `includegraphics` command you can use `\textwidth` which is the current width of the content block.

#### Listing 14: Adding Images

```
[...]  
35   \IPTgraphics[  
36     imgoptions={width=0.6\textwidth},  
37     caption={Caption of this picture},  
38     label=fig:rw_bcv,  
39     ]{img_2}  
[...]
```



## 2.8 Abstract

In case you want to add a short abstract to the poster, `tugPoster` provides a dedicated content block for this because the text of the abstract is slightly smaller and the the text is justified. To add an abstract simply use the environment `IPTabstractblock` similar to the previously explained `IPTblock`. `IPTabstractblock` does not support two-column text and should therefore be only used spanning one column of the whole poster.

### **Listing 15: Abstract block**

```
[...]
33 |     \begin{IPTabstractblock}{Abstract}
34 |         \lipsum[1]
35 |     \end{IPTabstractblock}
[...]
```



## **2.9 References**

Adding references to the poster requires two steps. First you need to add a content block using the `IPTrefsblock` environment. Similar to the abstract content block the references content block does not support the `twocolumn` option. The references block can be used either in a single column or spanning both columns.

Second, inside the `IPTrefsblock` use the environment `refs` to add your references. Every reference is a single `\item` inside the `refs` environment.

The contents of the references are automatically typeset in either two or three columns, depending on the width of the references block.

### **Listing 16: Nested two-column layout**

```
[...]
35 |     \begin{IPTrefsblock}{References}
36 |         \begin{refs}
37 |             \item \blindtext[2]
38 |             \item \blindtext[2]
39 |             \item \blindtext[2]
40 |             \item \blindtext[2]
41 |             \item \blindtext[2]
42 |             \item \blindtext[2]
43 |         \end{refs}
44 |     \end{IPTrefsblock}
[...]
```



## **2.10 Advanced Layouts**

### **2.10.1 Relative Lengths**

The `tugPoster` class supports different paper sizes. Depending on the paper size, the font size and all other layout elements (header, footer, etc.) adjusted. In case you

want to prepare your poster for different paper sizes and it is not sufficient to rely on measures such as `\textwidth`, additional lengths are provided:

`IPTRelWidth`: 1 % of the final page width, i.e. 8.41 mm for A0 or 5.94 mm for A1

`IPTRelHeight`: 1 % of the final page height, i.e. 11.89 mm for A0 or 8.41 mm for A1

This can be helpful for adjusting the size of images, etc., (see for example Listing 17)

### 2.10.2 Three Column Content

A special content block is the `\IPTcolorBlock3`. This content block provides three columns, each in its own minipage. Every column can be underlaid with some background color and between the header and the content every column can display an image. All three columns are of equal height and all three images are of equal height (and cropped in order to fill the available space).

`\IPTcolorBlock3` supports the following arguments:

`color1/color2/color3`: defines the background color for the three columns

`image1/image2/image3`: defines the image placed on top of every column

`imageHeight`: defines the height of the images (if used)

**Listing 17: Content block with thee columns**

```
[...]
43 \begin{IPTcolorBlock3}[
44   color2=gray!15!,
45   color3=gray!50!,
46   image1=hdr_left,
47   image2=hdr_middle,
48   image3=hdr_right,
49   imageHeight=10\IPTRelHeight,
50   ]{Header}

52 \IPTsection{Left Column}
53 \lipsum[1]

55 \IPTcolbreak

57 \IPTsection{Middle Column}
58 \lipsum[2]

60 \IPTcolbreak
[...]
```



### 2.10.3 Custom Institute Banner

In case you want to place a custom banner on the left-hand side of the poster instead of the institute's abbreviation the command `\IPTInstituteBanner` allows to place picture instead. If this command is used, the institute's short name is ignored.

#### Listing 18: Custom Banner

```
[...]
19 \IPTInstituteBanner{kurz_institute}
21 \begin{document}
22 [...]
```



### 2.10.4 Customizing Colors

The colors of the block headers and the color of the rectangle on the left-hand side above the institute's abbreviation can be customized with the commands `\IPTHeaderColor` and `\IPTInstituteColor`, see Listing 19

#### Listing 19: Custom Banner

```
[...]
29 \definecolor{IPTHeaderColor}{cmyk}{0,.96,.57,0}
30 \definecolor{IPTInstituteColor}{cmyk}{0,.36,1,0}
32 \begin{document}
33 [...]
```



## 2.11 Preparing for Print

If your printer does not support cutting the poster to the exact size or the printer leaves a certain margin around the poster, you can add either crop marks or a crop rectangle to the poster. This can be achieved by either adding the option `cropmarks` or `croprectangle` as documentclass option. If you add one of those options, also some meta-information such as the `\LaTeX` jobname, compilation date, etc., is added at the bleed.

The option `cropmarks` adds short lines slightly outside the final paper size while `croprectangle` additionally adds a thin rectangle at the page margins (see Figure 4).

### 3 Summary of Commands/Environments/Options

#### Document Class Options:

- `debug`: enables the debugging feature and highlights the bounding boxes of the content elements in different colors (see Section 5)
- `cropmarks`: produces a PDF that includes crop marks (and color bars) for cropping the printed poster
- `croprectangle`: same as `cropmarks` but with an additional rectangle at the poster's margins
- `size`: select the size of the poster. Currently A0 (default), A1, and 70x100 are supported

`IPTpartnersNote`: Adds a note to the footer. Typically used to give credits to sponsors and partners involved.

`IPTpartner`: Adds the logo of a partner to the footer. This command can be used multiple times

`IPTpartners`: Alternative to `\IPTpartner` if some special content needs to be added to the footer. (see Section 2.4)

`IPTHeaderColor`: Changes the color of all block headers. Needs to be defined via `\definecolor`, see Listing 19

`IPTInstituteColor`: Changes the color of rectangle on the left banner. Needs to be defined via `\definecolor`, see Listing 19. Not used if `IPTInstituteBanner` is set.

`IPTInstituteName`: Full name of the institute, printed at the poster's header.

`IPTInstituteAddress`: Full address of the institute, printed at the poster's header.

`IPTInstituteEmail`: General contact e-mail address, printed at the poster's header.

`IPTInstituteShort`: Abbreviation of the institute. printed at the banner on the left side. Not used if `IPTInstituteBanner` is set.

`IPTInstituteBanner`: Use a custom picture as banner on the left side.

`IPTInstituteURL`: Short URL of the institute's website. printed next to the QR-code in the footer. A full link to sub-page of the website can be specified via the optional first argument. Not used if `\NoQRCode` is used.

`NoQRCode`: Do not print the QR-code pointing to the institute's website in the footer

`ShowNFC`: Additionally print a NFC-logo below the QR-code in the footer if you provide additional information via an NFC-tag behind the poster.

**IPTblock:** Creates a basic content block.

Mandatory argument:

- Block Header: Headline of the content block

Optional argument:

- **twocolumn:** If specified the content block is split into two columns with a large gap between the two columns. Should be used for content blocks spanning the whole width.

**IPTwocol:** Separate the main layout into two columns. Shall only be used at the top level of the document with **IPTblock** elements as children. Produces a large gap between the two columns.

**IPTcols:** Allows to split the content into two columns having only a small gap between the two columns. Should be used either for content blocks spanning only one column of the whole poster, or nested in a column of a content block spanning the whole width.

Mandatory argument:

- Column width: fractional number between 0.0 and 1.0 specifying the width of the left column, typically 0.5.

**IPTabstractblock:** Variant of a basic content block **IPTblock** which uses a smaller font for the content. Should only be used when you want to add an abstract. Should only be used for a single column of the poster (i.e., **not** spanning the whole page width).

**IPTrefsblock:** Variant of a basic content block **IPTblock** which uses a smaller font for the block header and the content. Should only be used for adding a list of references to the poster. The references block can be used either for a single column of the poster or span the whole width.

**refs:** This environment is a specialized enumerate environment intended to list the references. Hence, this environment should always be used in combination with **IPTrefsblock**. Simply add each reference as a separate **\item**. The number of columns is automatically adjusted depending on the line width of the **\IPTrefsblock**

**\IPTgraphics:** Allows to easily add images. This command can be used similar to the commonly used **includegraphics** command. Using this command the image is horizontally centered within the current content column. Optionally you can specify a caption and a label.

Optional arguments:

- **imgoptions:** The argument for this option is directly passed on to the **includegraphics** command. This allows to adjust the size of the image, rotate the image or crop it.

- `caption`: Adds a caption to the image.
- `label`: Adds a label to the image which can be used with the `ref` command.

`\IPTcolbreak`: Adds a column break. All content elements after this command are added to the right column of the current element. Can be used within `IPTblock` (if the argument `twocol` is given), `IPTtwocol`, and `IPTcols`.

`\IPTsection`: Add further headlines within the `\IPTblock` content block.

`\IPTsubsection`: Add further headlines within the `\IPTblock` content block.

`IPTcolorBlock3`: Content block with three content columns. Each column can have a background color and an image on top of each column.

`IPTRelWidth`: 1 % of the final page width, i.e. 8.41 mm for A0 or 5.94 mm for A1

`IPTRelHeight`: 1 % of the final page height, i.e. 11.89 mm for A0 or 8.41 mm for A1

**Bullet lists:** for bullet lists the `itemize` environment can be used as usual up to a nesting level of three. The appearance of the list has been adapted to match the given layout.

## 4 Examples

`tugPoster` has been successfully used to create a poster containing itemized lists and many images. By nesting `IPTblock`, `IPTtwocol`, and `IPTcols` rather complex layouts can be realized as shown in Figure 1 and Figure 2.

## 5 Debugging / Layout Support

If you need to find out why a certain content element does not move further up or to the left/right it is often helpful to show the bounding boxes of the content elements. This can be achieved by adding the class option `debug` which shows the bounding box of every content element as well as the gaps between columns. `IPTtwocol` is shown in red, `IPTcols` is shown in green, and figures are shown in magenta (see Figure 3).

## 6 Known Issues

Currently there are no known issues. But in case you find some “misbehavior” feel free to contact the author with a detailed description ;-)

It would be nice to integrate `bibtex` for generating the references automatically. Maybe this will be added in a future version.

SCIENCE • PASSION • TECHNOLOGY

**TU**  
Graz

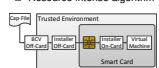
Institute for Technical Informatics ■ Infeldgasse 16/1, 8010 Graz, Austria ■ office@iti.tugraz.at

## Memory-Efficient On-Card Byte Code Verification for Java Cards

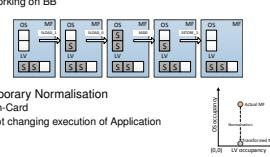
Reinhard Berlach, Michael Lackner and Christian Steger  
 Institute for Technical Informatics, Graz University of Technology  
 reinhard.berlach, michael.lackner, steger@tugraz.at

Johannes Loing and Ernst Haselsteiner  
 NXP Semiconductors  
 johannes.loing, ernst.haselsteiner@nxp.com

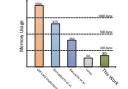
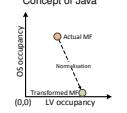
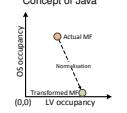
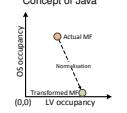
### Motivation

<p><b>Java Card Security</b> [7, 10]</p> <ul style="list-style-type: none"> <li>■ Bytecode           <ul style="list-style-type: none"> <li>■ Verification (BCV) [4, 8]</li> <li>■ Off-Card</li> <li>■ Resource intense algorithm</li> </ul> </li> </ul> 	<p><b>User Centric Ownership Model</b> [1]</p> <ul style="list-style-type: none"> <li>■ No Secure Loading</li> <li>■ No Business relationship between Card Supplier and Issuer</li> <li>■ Needs On-card BCV</li> </ul> 
--	--

### Memory-Efficient BCV

<ul style="list-style-type: none"> <li>■ Working on Basic Blocks           <ul style="list-style-type: none"> <li>■ Combining Normalising and CFG</li> <li>■ BB is smallest verifiable unit</li> </ul> </li> <li>■ Building CFG           <ul style="list-style-type: none"> <li>■ On-Card</li> <li>■ In linear time</li> <li>■ Reuse of Objects to minimize memory usage</li> </ul> </li> </ul> 	<ul style="list-style-type: none"> <li>■ Abstract Interpretation           <ul style="list-style-type: none"> <li>■ On-Card</li> <li>■ Working on BB</li> </ul> </li> <li>■ Temporary Normalisation           <ul style="list-style-type: none"> <li>■ On-Card</li> <li>■ Not changing execution of Application</li> </ul> </li> </ul> 
---	--

### Conclusion

<ul style="list-style-type: none"> <li>■ On-Card           <ul style="list-style-type: none"> <li>■ Algorithm running on-card</li> <li>■ Standard Compliance</li> </ul> </li> <li>■ Temporary Normalisation           <ul style="list-style-type: none"> <li>■ Reducing Memory consumption</li> <li>■ Usable also on low-cost Smart Cards</li> </ul> </li> </ul> 	<p><b>Related Work</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"> <p><b>Byte Code Verification</b></p> <ul style="list-style-type: none"> <li>■ Original BCV [4, 8]           <ul style="list-style-type: none"> <li>■ Off-Card</li> <li>■ Resource intense algorithm</li> <li>■ Abstract interpretation</li> <li>■ Part of the Sandbox Concept of Java</li> </ul> </li> </ul>  </td> <td style="width: 50%;"> <p><b>On Card BCV</b></p> <ul style="list-style-type: none"> <li>■ Proof Carrying Code (PCC) [9]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Verification in Single pass</li> <li>■ +50% size for PCC</li> </ul> </li> <li>■ Normalising [8]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Same memory consumption as execution</li> </ul> </li> <li>■ Reducing the Dictionary [2, 6]           <ul style="list-style-type: none"> <li>■ Using Control Flow Graphs</li> <li>■ Minimizing saved elements of Dictionary</li> </ul> </li> </ul> </td> </tr> </table>	<p><b>Byte Code Verification</b></p> <ul style="list-style-type: none"> <li>■ Original BCV [4, 8]           <ul style="list-style-type: none"> <li>■ Off-Card</li> <li>■ Resource intense algorithm</li> <li>■ Abstract interpretation</li> <li>■ Part of the Sandbox Concept of Java</li> </ul> </li> </ul> 	<p><b>On Card BCV</b></p> <ul style="list-style-type: none"> <li>■ Proof Carrying Code (PCC) [9]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Verification in Single pass</li> <li>■ +50% size for PCC</li> </ul> </li> <li>■ Normalising [8]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Same memory consumption as execution</li> </ul> </li> <li>■ Reducing the Dictionary [2, 6]           <ul style="list-style-type: none"> <li>■ Using Control Flow Graphs</li> <li>■ Minimizing saved elements of Dictionary</li> </ul> </li> </ul>
<p><b>Byte Code Verification</b></p> <ul style="list-style-type: none"> <li>■ Original BCV [4, 8]           <ul style="list-style-type: none"> <li>■ Off-Card</li> <li>■ Resource intense algorithm</li> <li>■ Abstract interpretation</li> <li>■ Part of the Sandbox Concept of Java</li> </ul> </li> </ul> 	<p><b>On Card BCV</b></p> <ul style="list-style-type: none"> <li>■ Proof Carrying Code (PCC) [9]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Verification in Single pass</li> <li>■ +50% size for PCC</li> </ul> </li> <li>■ Normalising [8]           <ul style="list-style-type: none"> <li>■ Needs Off-Card Components</li> <li>■ Same memory consumption as execution</li> </ul> </li> <li>■ Reducing the Dictionary [2, 6]           <ul style="list-style-type: none"> <li>■ Using Control Flow Graphs</li> <li>■ Minimizing saved elements of Dictionary</li> </ul> </li> </ul>		

**References**

- [1] R. Alten, K. Markatos, and K. Mayes. A Paradigm Shift in Java Card Verification. In *Proceedings of the Conference on Computational Science and Its Applications (CSCS)*, pages 1–8, 2002.
- [2] C. Berndsen, L. Martin, and P. Massi. Java bytecode normalisation for Java card verification. In *Proceedings of the Conference on Software Engineering and Applications (CSEA)*, pages 1–6, 2002.
- [3] D. Deville and C. Grimaud. Building an ‘impostor’ verifier for Java cards. In *Proceedings of the Conference on Industrial Experience with Systems Software. Volume 2, Software Engineering for Java Cards*, pages 111–118. IEEE, 1995.
- [4] J. Geling. Java intermediate bytecodes. *ACM SIGPLAN Notices*, 20(3):111–118, 1995.
- [5] X. Liang. Dynamic verification on Java smart cards.
- [6] R. Alten, K. Markatos, and K. Mayes. A Paradigm Shift in Java Card Verification. In *Proceedings of the Conference on Computational Science and Its Applications (CSCS)*, pages 1–8, 2002.
- [7] Oracle. Virtual Machine Specification. Java Card Platform, Version 2.2.1, 2002.
- [8] Oracle. Java card 3 platform off-card verification tool. February 2002.
- [9] Oracle. Java card 3 platform off-card verification tool. February 2002.
- [10] J. Geling and K. H. Rose. Lightweight Dynamic Verification. *Journal of Automated Reasoning*, 31:303–324, 2003.
- [11] J. Geling and K. H. Rose. Dynamic Verification of Java Card Programs. *Journal of Computer and Security Information*, 19(2):10–20, 2003.
- [12] J. Geling and K. H. Rose. Lightweight Dynamic Verification. *Journal of Automated Reasoning*, 31:303–324, 2003.
- [13] J. Geling and K. H. Rose. Lightweight Dynamic Verification. *Journal of Computer and Security Information*, 19(2):10–20, 2003.
- [14] X. Liang. Dynamic verification on Java smart cards.

Figure 1: Sample poster created with tugPoster showing a fancy layout.

**IVT**

SCIENCE • PASSION • TECHNOLOGY

Institut für Verbrennungskraftmaschinen und Thermodynamik | Inffeldgasse 19, 8010 Graz, Austria | emissions@ivt.tugraz.at

## Emissionsmessungen im realen Betrieb RDE – Real Driving Emissions

### Was ist RDE?

Als RDE werden REAL DRIVING EMISSIONS bezeichnet. Dabei werden die Emissionen eines Fahrzeugs On-Board im Straßenverkehr gemessen.

Die RDE-Messungen werden seit September 2017 für die Typisierung von neuen Fahrzeugtypen vorgeschrieben. Ab 2019 müssen alle PKW nach RDE zugelassen werden.

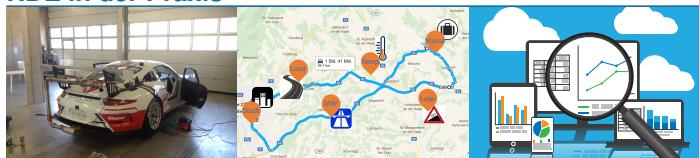
Neben der Messung der Emissionen am Prüfstand unter Laborbedingungen werden damit zusätzlich auch die Realfahrtmissionen des Fahrzeugs überprüft.

### Warum RDE?

Die bisherige Überprüfung, ob ein Fahrzeug die Emissionsgrenzwerte einhält, wurde in der Vergangenheit stark kritisiert. Fahrzeuge wurden auf den Typisierungszyklus hin optimiert und weisen im realen Betrieb teilweise ein anderes Emissionsverhalten auf.

Durch Messungen im realen Verkehr ist der Testablauf nicht mehr vorgegeben und die Fahrzeuge müssen in allen relevanten Situationen sauber sein.

### RDE in der Praxis



#### Installation

Das PEMS (Portable Emission Measurement System) muss im oder am Fahrzeug installiert werden.

#### RDE-Messung

Die Emissionsmessung findet unter Vorgabe von bestimmten Randbedingungen im realen Betrieb des Fahrzeugs auf der Straße statt.

#### Datenanalyse

Die Datenanalyse zeigt, ob die Messfahrt gültig war und die RDE-Emissionen werden berechnet.

#### Komponenten PEMS

- Analysatoren für die Messung der Schadstoffkomponenten
- GPS und mobile Wetterstation
- Exhaust Fuel Meter für die Messung des Abgasmassenstroms

#### Checkliste für die Installation

- Eigene Energieversorgung
- Kalibrierung der Messgeräte vor Messantritt
- Validierung der Messgeräte mit Labormessung als Referenz

#### Randbedingungen RDE-Fahrt

- Streckenanteile für Stadt, Land und Autobahn
- Gesamtdauer der Messfahrt
- Durchschnittliche Geschwindigkeiten, Stop-Zeiten
- Maximale und minimal erlaubte Dynamik der Messfahrt

#### Einflussfaktoren

- Verkehrsaufkommen
- Wetterverhältnisse
- Fahrstil (aggressiv oder ökonomisch)
- Geografische Lage der gewählten Route (Seehöhe)

#### Auswertungen

- Einhaltung der Limits für RDE
- Analyse eventueller Schwachpunkte eines Kfz bezüglich Emissionen
- Entwicklung von Simulationsmodellen der vermessenen Kfz
- Simulation des Emissionsverhaltens der Kfz

---

### Kontakt

Ao. Univ.-Prof. Dr. Stefan Hausberger  
Inffeldgasse 19  
8010 Graz, Austria  
Tel.: +43 316 873 30260  
Fax.: +43 316 873 30262  
Mail: hausberger@ivt.tugraz.at





www.ivt.tugraz.at

Figure 2: Sample poster created with tugPoster showing a fancy layout.

**ITI**

**TU** **Graz**  
SCIENCE • PASSION • TECHNOLOGY

Institute for Technical Informatics ■ Infeldgasse 16/1, 8010 Graz, Austria ■ office@iti.tugraz.at

## Memory-Efficient On-Card Byte Code Verification for Java Cards

Reinhard Berlach, Michael Lackner and Christian Steger  
Institute for Technical Informatics, Graz University of Technology  
reinhard.berlach, michael.lackner, steger@tugraz.at

Johannes Loing and Ernst Haselsteiner  
NXP Semiconductors  
johannes.loing, ernst.haselsteiner@nxp.com

### Motivation

#### Java Card Security [7, 10]

- Bytecode
  - Verification (BCV) [4, 8]
  - Off-Card
  - Resource intense algorithm

**Secure Loading**

- Off and On-Card Component
- Done by Cryptographic Signature
- Key-exchange between Card Supplier and Issuer

**User Centric Ownership Model [1]**

- No Secure Loading
- No Business relationship between Card Supplier and Issuer
- Needs On-card BCV

**Overview of the User Centric Ownership Model [1]**

### Memory-Efficient BCV

#### Working on Basic Blocks

- Combining Normalising and CFG
- BB is smallest verifiable unit

#### Building CFG

- On-Card
- In linear time
- Reuse of Objects to minimize memory usage

#### Abstract Interpretation

- On-Card
- Working on BB

#### Temporary Normalisation

- On-Card
- Not changing execution of Application

### Conclusion

#### On-Card

- Algorithm running on-card
- Standard Compliance

#### Temporary Normalisation

- Reducing Memory consumption
- Usable also on low-cost Smart Cards

### Related Work

#### Byte Code Verification

#### On Card BCV

- Proof Carrying Code (PCC) [9]
  - Needs Off-Card Components
  - Verification in Single pass
  - ~50% size for PCC
- Original BCV [4, 8]
  - Off-Card
  - Resource intense algorithm
  - Abstract interpretation
  - Part of the Sandbox Concept of Java
- Normalising
  - Needs Off-Card Components
  - Same memory consumption as execution
- Reducing the Dictionary [2, 6]
  - Using Control Flow Graphs
  - Minimizing saved elements of Dictionary

**References**

- [1] R. Alten, K. Markatoska, and K. Meier. A Paradigm Shift in Java Card Security. In Proceedings of the International Conference on Computational Science and Its Applications (CICS'02), volume 2313 of Lecture Notes in Computer Science, pages 100–111. Springer, 2002.
- [2] C. Berndesdorff, L. Martin, and P. Maes. Java bytecode normalisation for Java Card. In Proceedings of the International Conference on Software Engineering and Applications (ICSEA'05), volume 2, pages 11–16. IEEE, 2005.
- [3] D. Deville and C. Grimaud. Building an ‘impostor’ verifier for Java Card. In Proceedings of the International Conference on Industrial Experiences with Systems Software - Volume 2, Software Engineering for Industrial Applications (SEIA'05), pages 111–118. ACM SIGPLAN, 2005.
- [4] J. Giesking. Java intermediate bytecodes. ACM SIGPLAN Notices, 30(11):111–118, 1995.
- [5] X. Liang. BCV verification on Java smart cards.
- [6] D. Mandrić, A. Tsvetkov, C. Tronche, and E. Tsigas. Reducing the memory complexity of type inference. In Proceedings of the International Conference on Formal Methods in Computer Security, volume 2513 of Lecture Notes in Computer Science, pages 150–164. Springer, 2002.
- [7] Oracle. Virtual Machine Specification. Java Card Platform, version 2.2.1, 2007.
- [8] Oracle. Java card 3 platform off-card verification tool. Oracle Platform 2007, 2007.
- [9] P. Rohr and K. H. Rose. Lightweight Bytecode Verification. Journal of Automated Reasoning, 31:301–334, 2003.
- [10] J. Giesking. Java Card Security. Information Security Bulletin, July 2005.

**www.iti.tugraz.at**

Figure 3: Sample poster with the debug option enabled.

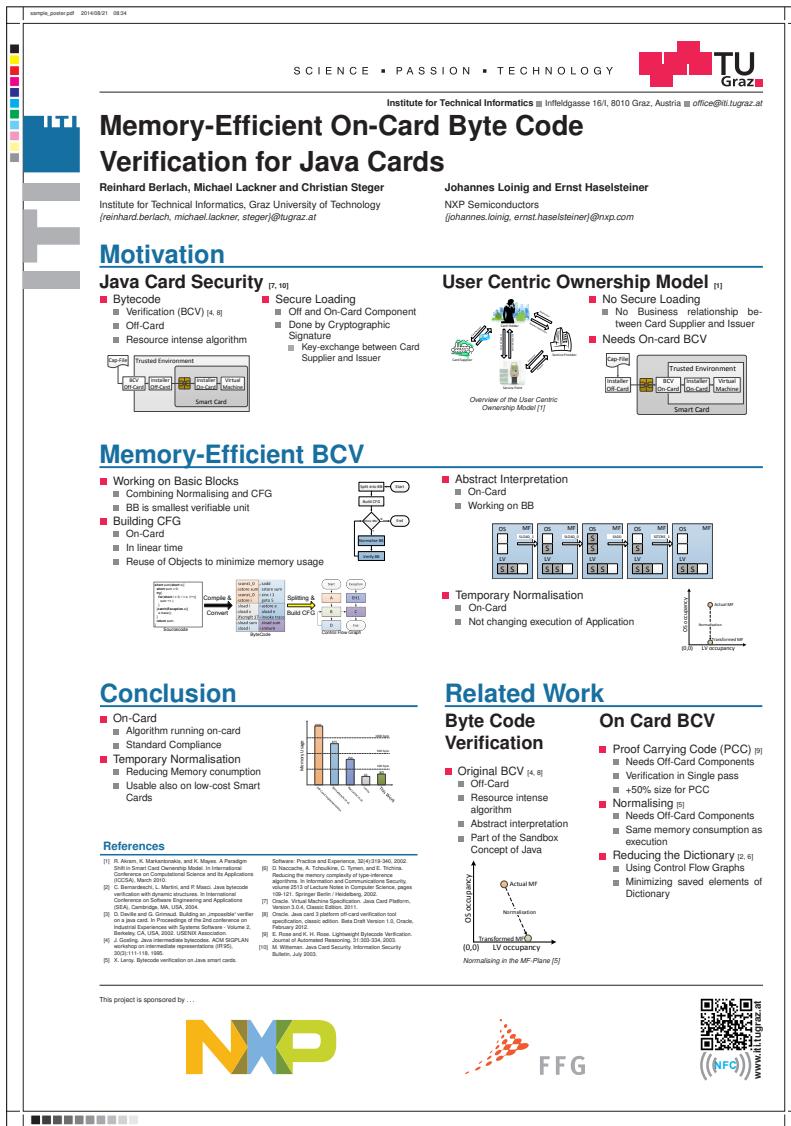


Figure 4: Sample poster with a “crop rectangle” ready to print and easy cutting.