北京航空航天大學

BEIHANG UNIVERSITY

第三十三届“冯如杯”竞赛主赛道项目论文模板

——基于 Latex 的论文模板

摘要

本 Latex 模板是北京航空航天大学大学第三十三届“冯如杯”竞赛主赛道论文模板，由北京航空航天大学校团委基于 GitHub 用户 ***Somedaywilldo*** 与 ***cpfy*** 的成果迭代开发而来。在此由衷感谢所有开发者对本模板的贡献与对“冯如杯”竞赛的大力支持。

摘要内容包括：“摘要”字样，摘要正文，关键词。在摘要的最下方另起一行，用显著的字符注明文本的关键词。

摘要是论文内容的简短陈述，应体现论文工作的核心思想。摘要一般约 500 字。摘要内容应涉及本项科研工作的目的和意义、研究思想和方法、研究成果和结论。

关键词是为用户查找文献，从文中选取出来用来揭示全文主题内容的一组词语或术语，应尽量采用词表中的规范词（参照相应的技术术语标准）。关键词一般为 3 到 8 个，按词条的外延层次排列。关键词之间用逗号分开，最后一个关键词后不打标点符号。

关键词：关键词 1，关键词 2，关键词 3，关键词 4，关键词 5

Abstract

This Latex template for the 33rd Fengru Cup Competition of Beihang University, is developed by Communist Youth League Committee of BUAA iteratively based on the contribution of GitHub users ***Somedaywilldo*** and ***cpfy***. Here, we would like to thank all the developers for their contributions to this template and for their support of the Fengru Cup Competition.

The abstract includes: the word "Abstract", the body of the abstract, and the keywords. On a separate line at the bottom of the abstract, indicate the key words of the text in prominent characters.

The abstract is a short statement of the content of the paper and should reflect the core ideas of the paper work. The abstract is usually about 500 words. The abstract should cover the purpose and significance of this scientific work, research ideas and methods, research results and conclusions.

Keywords are a set of words or terms selected from the text to reveal the subject content of the whole text for the user to find the literature, and the standardized words in the word list (refer to the corresponding technical terminology standards) should be used as much as possible. The keywords are usually 3 to 8, arranged according to the level of extensibility of the words. The keywords are separated by commas, and no punctuation marks are used after the last keyword.

Keywords: Keywords 1, Keywords 2, Keywords 3, Keywords 5, Keywords 6

目录

一、简介

第三十三届“冯如杯”主赛道论文一律由在计算机上输入、排版、定稿后转成 PDF 格式，在集中申报时通过网络上传。**论文封面及全文中不能出现作者姓名、学院、专业、指导老师的相关信息**。包括 5 个部分, 顺序依次为:

- 封面（中文）
- 中文摘要、关键词 (中文、英文)
- 主体部分
- 结论
- 参考文献

二、论文的书写规范

论文正文部分需分章节撰写，每章应另起一行。章节标题要突出重点，简明扼要、层次清晰。字数一般在 15 字以内，不得使用标点符号。标题中尽量不采用英文缩写词，对必须采用者，应使用本行业的通用缩写词。层次以少为宜，根据实际需要选择。三级标题的层次按章（如“一、”）、节（如“(一)”）、条（如“1.”）的格式编写，各章题序的阿拉伯数字用 Times New Roman 体。

（一）字体和字号

论文题目：二号，华文中宋体加粗，居中。

副标题：三号，华文新魏，居右（可省略）。

章标题：三号，黑体，居中。

节标题：四号，黑体，居左。

条标题：小四号，黑体，居左。

正文：小四号，中文字体为宋体，西文字体为 Times New Roman 体，首行缩进，两端对齐。

页码：五号 Times New Roman 体，数字和字母

（二）页边距及行距

学术论文的上边距：25mm；下边距：25mm；左边距：30mm；右边距 20mm。章、节、条三级标题为单倍行距，段前、段后各设为 0.5 行（即前后各空 0.5 行）。正文为 1.5

倍行距，段前、段后无空行（即空 0 行）。

（三）页眉

页眉内容为北京航空航天大学第三十三届“冯如杯”竞赛主赛道参赛作品，内容居中。页眉用小五号宋体字，页眉标注从论文主体部分开始（引言或第一章）。请注意论文封面无页眉。

（四）页码

论文页码从“主体部分（引言、正文、结论）”开始，直至“参考文献”结束，用五号阿拉伯数字连续编码，页码位于页脚居中。**封面、题名页不编页码**。

摘要、目录、图标清单、主要符号表用五号小罗马数字连续编码，页码位于页脚居中。

（五）图、表及其附注

图和表应安排在正文中第 1 次提及该图、表的文字的下方，当图或表不能安排在该页时，应安排在该页的下一页。

1. 图

图题应明确简短，**用五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，图的编号与图题之间应空半角 2 格。图的编号与图题应置于图下方的居中位置。图内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。曲线图的纵横坐标必须标注“量、标准规定符号、单位”，此三者只有在不必要注明（如无量刚等）的情况下方可省略。坐标上标注的量的符号和缩略词必须与正文中一致。

2. 表

表的标号应采用从 1 开始的阿拉伯数字编号，如：“表 1”、“表 2”、……。表编号应一直连续到附录之前，并与章、节和图的编号无关。只有一幅表，仍应标为“表 1”。表题应明确简短，用**五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，表的编号与表题之间应空半角 2 格。表的编号与表头应置于表上方的居中位置。表内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。

3. 附注

图、表中若有附注时，附注各项的序号一律用“附注 + 阿拉伯数字 + 冒号”，如：“附注 1：”。

附注写在图、表的下方，一般采用 5 号宋体。

4. 参考文献

凡有直接引用他人成果（文字、数字、事实以及转述他人的观点）之处，均应加标注说明列于参考文献中，以避免论文抄袭现象的发生。

标注格式：引用参考文献标注方式应全文统一，标注的格式为 [序号]，放在引文或转述观点的最后一个句号之前，所引文献序号用小 4 号 Times New Roman 体、以上角标形式置于方括号中，如“……成果”[1]。

三、原理与算法

（一）基于哈达玛积的问题转化

（二）基于交互式谕示机证明的零知识范围证明

1. 默克尔树

默克尔树（Merkle Tree or Hash Tree）是一棵用哈希值搭建起来的树，树的所有节点都存储了哈希值。整棵树包含根节点、中间节点和叶节点。树采取自下而上的生成方式，叶节点经哈希运算得到哈希值，而其余节点的哈希值均由其子节点的哈希值经哈希计算得到。默克尔树的具体结构见**??**Merkle。

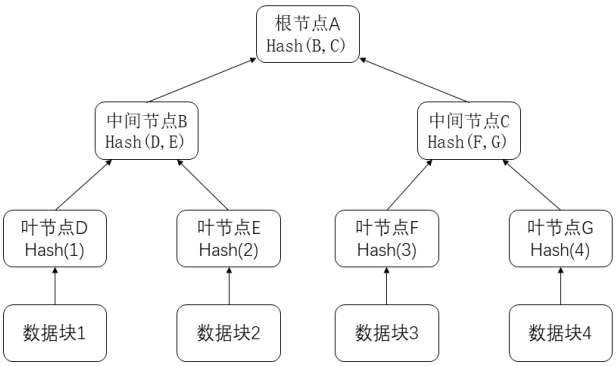


图 1 默克尔树结构图

基于哈希函数的防碰撞特性（Collision resistance）、隐藏性 (Hiding) 和谜题友好性（Puzzle friendly），对默克尔树的任意局部修改，都会对根节点和路径上的中间节点产生影响。默克尔树的这个特性提供了一种很好的检测数据是否被篡改的方法。在本文中，我们使用具有抗碰撞特性和不可逆特性的哈希函数来构造默克尔树，进而利用构造的树

来完成对向量的承诺，并通过次线性尺度的证明来开放树的多处索引。对向量 v 的承诺包含以下三种算法，即承诺操作（Commit）、开放操作（Open）、验证操作（Verify）：

- $\text{root}_v \leftarrow \text{MT.Commit}(v)$
- $(\{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v) \leftarrow \text{MT.Open}(\mathcal{I}, v)$
- $\{1, 0\} \leftarrow \text{MT.Verify}(\text{root}_v, \mathcal{I}, \{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v)$

2. 里得 · 所罗门编码

里得 · 所罗门编码（Reed-Solomon Code, RS Code）是一种编码方式，用其编码的码字是域上某个特定单变量多项式的一组函数值，表示成向量的形式。因此，在本文中我们使用 RS Code 来编码向量。

用抽象代数的模型来定义，选择一个 q 阶的有限域 $\mathbb{F}$，作为编码的字母表。再选择 $\mathbb{F}$ 的一个陪集 L，所选择的特定单变量多项式成为编码多项式（encoding polynomial），且度小于 $\rho \cdot |L|$，其中 $\rho \in (0, 1)$ 称为编码率，用这样的多项式编码出的向量表示为 $\text{RS}[L, \rho] \in \mathbb{F}^{|L|}$。

具体而言，编码的过程如下：设插值集 $H = \{\xi_1, \cdots, \xi_{|H|}\}$，估值集 $L = \{\eta_1, \cdots, \eta_{|L|}\}$，且 $|L| > |H|$，被编码的向量设为 $v \in \mathbb{F}^{|H|}$。首先，找到预设的度的编码多项式 $\hat{p}$，使得 $\hat{p}|_H = \{\hat{p}(\xi_1), \cdots, \hat{p}(\xi_{|H|})\} = v$。然后计算 $\hat{p}$ 在 L 上的估值（Evaluation），得到码字 $\hat{p}|_L$。计算估值和插值的算法使用快速傅里叶变换（Fast Fourier Transform, FFT）和其逆变换（IFFT）。

3. 诚实验证方前提的零知识证明

零知识证明（Zero-Knowledge Argument of Knowledge, ZKAoK）是一种验证协议，在其中证明方（Prover）不提供任何有关某个论断的有用信息，而能使验证方（Verifier）验证该论断为正确的。这项协议技术在信息安全及密码学等领域应用广泛。“诚实验证方前提（Honest Verifier）”意为验证方是正确遵循协议进行验证的。

用计算复杂度理论（Computational Complexity Theory）的模型定义，零知识证明是一个用于证明 NP（Non-deterministic Polynomial）二元关系 $\mathcal{R}$ 的算法三元组 $(\mathcal{G}, \mathcal{P}, \mathcal{V})$。其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示非确定多项式时间（Probabilistic Polynomial Time, PPT）的证明算法和验证算法。

诚实验证方前提的零知识证明具有以下条件需要满足：

- **完备性（*Completeness*）**：即正确的论断都可以被证明为正确。假设 λ 为私有参数，对于每个 $\mathcal{G}$ 的输出 pp$\leftarrow \mathcal{G}(1^\lambda)$，每个 $\mathcal{R}$ 中的元素 (x, ω)，以及字母表上任意字符

串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}(\omega), \mathcal{V}(z)(\text{pp}, x) = 1\rangle] = 1 - \text{negl}(\lambda)$$

其中 Pr 表示概率，negl(λ) 表示当 λ 足够大时，可以忽略不计的量。

- **正确性（*Soundness*）**：即被证明的论断大都是正确的，只有极小的可能出错。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，每个不在 $\mathcal{R}$ 中的元素 (x, ω)，以及字母表上任意字符串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}(z)(\text{pp}, x) = 1\rangle] \leq \text{negl}(\lambda)$$

其中 $\mathcal{P}^*$ 表示任意的 PPT 证明方。

- **零知识性（*Zero-knowledge*）**：即 $\mathcal{P}$ 和 $\mathcal{V}$ 之间的对话可以只依据公开信息被完全模拟。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，任意的诚实的 PPT 验证方 $\mathcal{V}$，每个 $\mathcal{R}$ 中的元素 (x, ω) 和任意字母表上的字符串 $z \in \{0,1\}^*$，存在一个 PPT 模拟机 $\mathcal{S}$，使得：

$$\{\langle \mathcal{P}(\omega), \mathcal{V}(z)\rangle(\text{pp}, x)\} \overset{c}{\approx} \{\mathcal{S}^{\mathcal{V}}(\text{pp}, x, z)\}$$

其中 $\mathcal{S}^{\mathcal{V}}$ 表示多项式空间下给定 $\mathcal{V}$ 的模拟机，$\overset{c}{\approx}$ 表示两者在计算上不可区分（Computationally indistinguishable）。

- **知识论证性（*Argument of knowledge*）**：即所有论证的证明都不会是不合法的。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，任意的 $x, z \in \{0,1\}^*$，对于所有恶意的 PPT 证明方 $\mathcal{P}^*$，存在一个可预期多项式时间的抽取机 $\mathcal{E}$，使得：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}(z)\rangle(\text{pp}, x) = 1 \wedge ((x, \omega) \notin \mathcal{R})|_{\omega \leftarrow \mathcal{E}^{\mathcal{P}^*}(\text{pp}, x)}] \leq \text{negl}(\lambda)$$

其中 $\mathcal{E}^{\mathcal{P}^*}$ 表示抽取机对 $\mathcal{P}^*$ 的任意性及整个运行过程都具有访问权限。

4. 交互式谕示机证明

交互式谕示机证明（Interactive Oracle Proof, IOP）是一种证明系统模型，在其中验证方可以通过谕示机概率性地问询证明方所持有的关于被证明的论断的有效信息，但由于是概率性地问询，所以验证方并不能得到证明方的全部信息。

同样，使用计算复杂度理论的模型来定义，IOP 是证明 k 轮 NP 二元关系的算法

三元组 $(\mathcal{G},\mathcal{P},\mathcal{V})$，其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示 PPT 证明算法和验证算法。具体而言，一个 k 轮的 IOP 包含 k 轮的交互（interaction）。在第 i 轮（$0<i\leq k$），验证方向证明方均匀且随机地发送消息 m_i，且验证方能够通过谕示机得到以 m_i 为输入的输出，证明方需返回 π_i 给验证方。在最后一轮，验证方得到了证明方返回的 k 个位置的信息 $\pi=(\pi_1,\cdots,\pi_k)$，并且需决定接受或拒绝证明方的证明（Proof）。

交互式谕示机证明具有以下条件需要满足：

- **完备性（*Completeness*）**：对于每个 $\text{pp}\leftarrow\mathcal{G}(1^\lambda)$ 以及 $(x,\omega)\in\mathcal{R}$，有：

$$\Pr[\langle\mathcal{P}(\omega),\mathcal{V}^\pi\rangle(\text{pp},x)=1]=1$$

  其中 $\mathcal{V}^\pi$ 表示 $\mathcal{V}$ 可以访问谕示 π。

- **正确性（*Soundness*）**：对于每个 $\text{pp}\leftarrow\mathcal{G}(1^\lambda)$，每个 PPT 的 $\mathcal{P}^*$ 以及 $(x,\omega)\notin\mathcal{R}$，有：

$$\Pr[\langle\mathcal{P}^*(\omega),\mathcal{V}^\pi\rangle(\text{pp},x)=1]\leq\text{negl}(\lambda)$$

在本文中所应用的原理中，主要涉及两种类型的 IOP，分别是 *RS-IOP* 和 *IOP of proximity*，前者即使用里德-所罗门码（Reed-Solomon code）的 IOP，后者指对于正确性的条件，允许证明方的秘密和合法证据之间具有微小的差距（proximity）。

5. 单变量求和校验协议

单变量求和校验协议（Univariate Sum-check Protocol）主要应用于有限域上的多项式求和问题。首先，假设有两个乘法群 $H,L\subset\mathbb{F}$ $(|L|>|H|)$，一个小于 $k(k>|H|)$ 阶的单变量多项式 $f(\cdot)$，以及一个被声明（claimed）的和 μ。在已有假设上，单变量求和校验协议的作用就是证明 $\sum_{a\in H}f(a)=\mu$。在实际操作中，证明方需要将 $f(x)$ 利用带余除法唯一地转化为 $x\cdot\hat{p}(x)+\zeta+\hat{Z_H}(x)\hat{h}(x)$，其中除式为 $\hat{Z_H}(x)$，代表 H 上的“消失”多项式（Vanishing polynomial），满足 $\forall a\in H,\ \hat{Z_H}(a)=0$。接着，基于对 $\hat{f}|_L$ 和 $\hat{h}|_L$ 的谕示机访问，验证方可以验证是否有 $\hat{p}|_L\in\text{RS}(L,\frac{|H|-1}{|L|})$ 以及 $\hat{h}|_L\in\text{RS}(L,\frac{|L|-|H|}{|L|})$，其中 $\hat{p}(x)=\dfrac{|H|\cdot\hat{f}(x)-\mu-|H|\cdot\hat{Z_H}(x)\hat{h}(x)}{x}$。这种基于 RS 编码加密的 IOP 具有完美的完整性和完美的完备性。当我们将它转换为一个 IOP 时，它仍然是在检验谕示 $\hat{f}|_L,\hat{h}|_L,\hat{p}|_L$ 是否为具有相应度的界限的 RS 码。而这个过程可以通过下面的低度检测协议来完成。

6. 低度检测和 FRI

给定度 $k_1, \cdots, k_t$，码字 $\hat{v}_1|_L, \cdots, \hat{v}_t|_L$，其中 L 为一个乘法陪集，低度检测协议允许验证方借助对这些码字的谕示机访问来检验以下语句是否成立：

$$\forall j \in \{0, \cdots, t\},\ \hat{v}_j|_L \in \mathbf{RS}[L, \frac{k_j}{|L|}]$$

即用于编码给定码字的编码多项式的度是否低于给定的度。

在本文中，我们的低度检测协议选取快速 Reed-Solomon 交互式谕示机邻近证明（Fast Reed-Solomon Interactive Oracle Proof of Proximity, Fast RS IOPP, FRI）。给定对证明方消息 l 处取值的谕示机访问，该 FRI 是具有完整性（Completeness）和正确性（Soundness）容错率为 $O(\frac{L}{\mathbb{F}}) + \mathrm{negl}(l, k)$ 的 IOPP，其中 $l = O(\lambda), k = \max\{k_1, \cdots, k_t\}$。

总的来说，用于实现单变量求和校验的 FRI 协议可以表示为：

$$\langle \mathrm{FRI}.\mathcal{P}(\hat{f}, \hat{h}, \hat{p}, \mathrm{FRI}.\mathcal{V}^{\hat{f}|_L, \hat{h}|_L, \hat{p}|_L}) \rangle (k, k - |H|, |H| - 1)$$

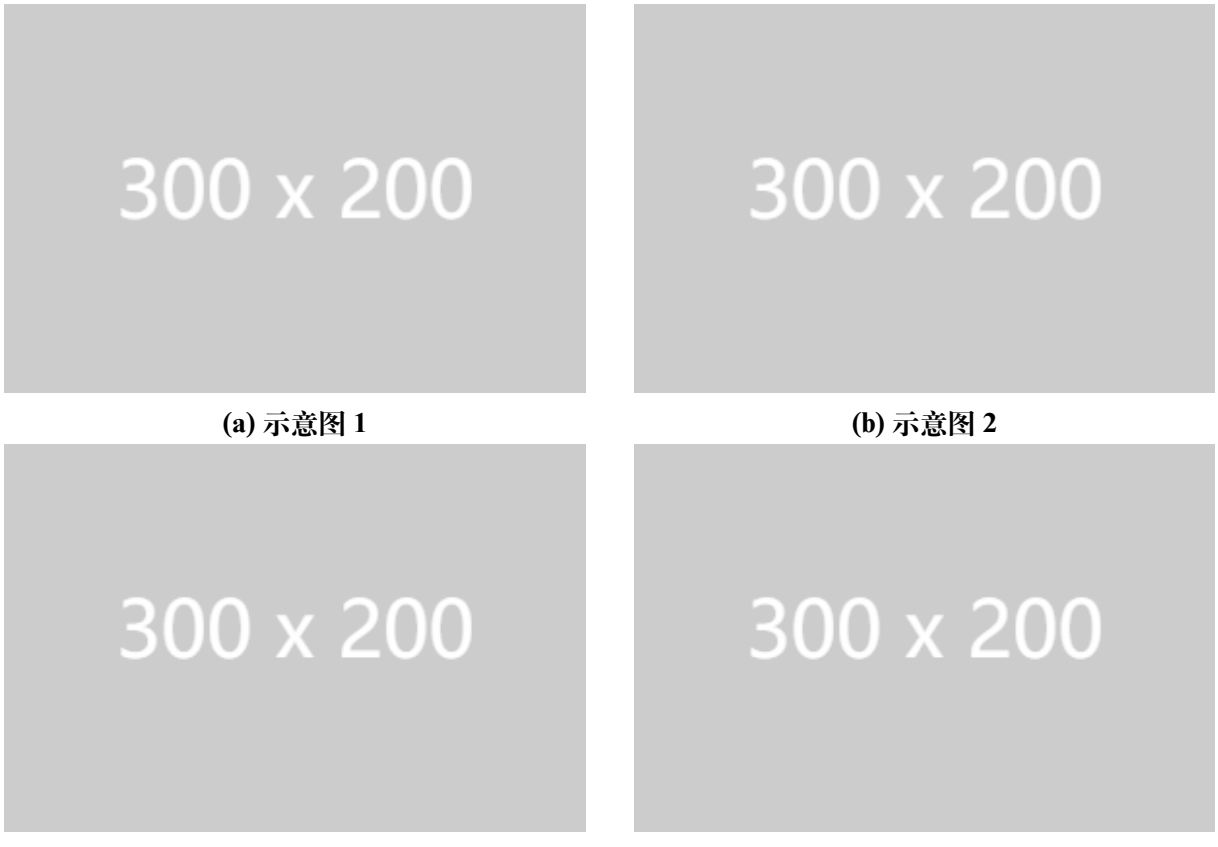
四、图表模板

图表示例展示如下：

图 2 example_caption

(a) 示意图 1 **(b) 示意图 2** **(c) 示意图 3**

图 3 一行三张子图并排示意



(a) 示意图 1 **(b) 示意图 2**

(c) 示意图 3 **(d) 示意图 4**

图 4 2*2 四张子图示意

表 2 三线表使用示例

方法	表头 1	表头 2	表头 3	表头 4
方法 1	数据	数据	数据	数据
方法 2	数据	数据	数据	数据

结论

论文的结论单独作为一章，但不加章号。

注意: 文件大小不超过 5M。

参考文献

[1] 张志建. 严复思想研究 [M]. 桂林：广西师范大学出版社，1989.

[2]（英）霭理士. 性心理学 [M]. 潘光旦译. 北京：商务印书馆，1997.

[3] 伍蠡甫. 西方论文选（下册）[C]. 上海：上海译文出版社，1979.

[4] 叶朗. 《红楼梦》的意蕴 [J]. 北京大学学报（哲学社会科学版），1989，(2)

[5] 谢希德. 创造学习的新思路 [N]. 人民日报，1998-12-25（10）

[6]Mansfeld, R.S. & Busse. *T.V. The Psychology of creativity and discovery*, Chinago：NelsonHall, 1981