HZ BOOKS
华章科技

C/C++
技术丛书

C指针原理揭秘
基于底层实现机制

刘兴 编著

Theory of C Pointer
Core Implementation Mechanism

- 理论结合实践，从C指针原理、C语言核心双角度进行深入剖析，使读者更好地把握C指针这把双刃剑，避免C指针给编程者带来的无所适从感，跳出内存泄漏、指针越界、指针类型错误等陷阱。

机械工业出版社
China Machine Press

C/C++
技术丛书

C指针原理揭秘

基于底层实现机制

Theory of C Pointer
Core Implementation Mechanism

刘兴 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

C 指针原理揭秘：基于底层实现机制 / 刘兴编著 . —北京：机械工业出版社，2019.5
（C/C++ 技术丛书 ）

ISBN 978-7-111-62683-1

I. C… II. 刘… III. C 语言 - 程序设计 IV. TP312.8

中国版本图书馆 CIP 数据核字（2019）第 083514 号

指针是 C 语言中广泛使用的一种数据类型，是 C 语言中功能强大而又让人迷惑的亮点，运用指针编程是 C 语言最主要的风格之一。本书力求从底层实现机制进行解析，同时配合 C/C++ 编程技巧以及某些指针运用技巧，讲解如何提高程序效能，如何避免滥用指针。全书分为准备篇、基础篇和进阶篇。准备篇介绍 C 语言、开发环境搭建以及 AT&T 汇编；基础篇对指针基础及 C 开发基础进行介绍；进阶篇讲述 C 开发技巧、C 并行与网络基础等高级主题。

C 指针原理揭秘：基于底层实现机制

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：冯秀泳　　责任校对：殷　虹
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2019 年 5 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：16.5
书　　号：ISBN 978-7-111-62683-1　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

Preface 前　言

为什么要写这本书

C 语言是一种计算机程序设计语言，它既具有高级语言的特点，又具有汇编语言的特点。它由美国贝尔实验室的 D. M. Ritchie 于 1972 年推出。1978 年后，C 语言已先后被移植到大、中、小及微型机上。它可以作为工作系统设计语言，编写系统应用程序；也可以作为应用程序设计语言，编写不依赖计算机硬件的应用程序。它的应用范围广泛，适用于系统软件开发及嵌入式开发领域，具备很强的数据处理能力，不仅仅是在软件开发上，在各类科研中也都需要用到 C 语言。

指针是 C 语言中广泛使用的一种数据类型，是 C 语言中功能强大而又让人迷惑的亮点，运用指针编程是 C 语言最主要的风格之一。作为一把双刃剑，C 指针让 C 语言成了能编写操作系统的接近硬件层的语言，能让编程者实现很多其他语言实现不了的功能；但是有时编程者也会感到无所适从，因为稍有不慎，就将造成内存泄漏、指针越界、指针类型错误等异常情况。而汇编中间码揭示了内存如何分配和使用、翻译形成的底层语言如何工作等，通过分析汇编中间码，揭开隐藏在 C 语言背后的秘密，剖析“C 指针作为内存里的一个地址”这一事实。

C 指针本质及其实现机制非常重要，为了让编程者更好地掌握这把“双刃剑”，本书从指针基础讲解入手，由浅入深，最后分析了汇编及底层语言，全面剖析了 C 指针。

读者对象

- 程序员。C/C++ 程序员能在充分理解 C 指针以及指针实现机制的基础上，开发软件系统的中间件、核心库，评估内存占用、运行效率、突发异常、程序后门等情况，提高

软件质量，增加可移植性，进行编译优化；而对占用 CPU 时间较多的代码可用汇编语言代替，提高软件运行速度。在受限环境（嵌入开发、并行计算、冗余系统等）下，正确使用 C 指针以及评估软件运行质量，能促使编写的代码更稳定、更安全、更高效。脚本语言程序员也能从 C 指针中收获很多，Python、Perl 等脚本语言都能与 C/C++ 混合编程。

- 架构师。指针是 C/C++ 语言的基石，任何复杂的算法和大型甚至云计算软件系统都是基于这些基石构造的，只有掌握好系统的底层，才能提高系统整体运行效率。架构师在理解 C/C++ 指针以及实现机制的基础上，能根据软件运行环境定制适合软件需求的架构，每种软件架构在内存分配、程序运行等方面都有自己的使用策略。目前，随着大数据时代的来临，云计算平台发展很快，C/C++ 语言编程质量的改进能提高云计算中单机的运行效率和稳定性，能优化数据在云计算网络的传输效率。
- 算法工程师。近年来，随着国内计算机行业的发展，数据挖掘、机器学习、算法工程、云计算、编译工程、芯片工程等新生事物相继出现，这些以前仅在高校和科研院所研究的技术需要算法工程师的努力才能成为现实，而掌握诸如指针等编程知识是实现算法的基础。

如何阅读本书

全书分为准备篇、基础篇、进阶篇。指针及相关内容是编程语言中较难理解的部分，脚本语言稍好些，C/C++ 语言中会更加明显。虽然理解指针本身并不复杂，但指针之间的组合以及指针的灵活运用却存在不同的技巧，不同的组合能产生不同的效果，也有着不同的作用。本书力求从底层实现机制进行解析，同时配合 C/C++ 编程技巧以及某些指针运用技巧，讲解如何提高程序效能，如何避免滥用指针。

本书首先从在 C 语言编程的角度讲解 C 指针，力图使读者学会运用 C 指针进行开发，并能进一步灵活将指针运用在精巧的算法上，构造更复杂的软件系统。

接着，对 C 语言标准进行讲述。C 语言属于高级语言，广泛采用的有 C89 和 C99 这两个主要标准。C89 于 1989 年以 ANSI X3.159—1989“ Programming Language C”名称发布生效，这个版本的语言经常被称作 ANSI C，或 C89；C99 在 C89 的基础上新增了一些特性，作为 C 语言官方标准的第 2 版，于 1999 年以 ISO/IEC 9899:1999“ Programming Language-C”名称发布生效，并于 2000 年 3 月被 ANSI 采纳。

最后，对编译器的实现原理进行解读。编译器对 C 语言进行编译，编译后形成可执行文

件，针对 C/C++ 语言以编译的形式执行（TCC 等提供了一种解释执行 C 脚本的方式，但其原理和编译执行差不多）的情况，重点从编译器生成的汇编中间码对指针进行剖析。

勘误和支持

由于作者的水平有限，编写的时间也很仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。你在遇到任何问题或有更多的宝贵意见时，欢迎发送邮件至我的邮箱 liu.xing.8@foxmail.com，很期待能够听到你的真挚反馈。此外，本书的代码及相关资源请在网盘（网盘地址：https://dwz.cn/uo3gCxWK，提取码：457a）下载，本书读者 QQ 群为 834755376。

致谢

在此，我衷心感谢机械工业出版社华章公司编辑杨福川老师和策划编辑杨绣国老师，由于他们的魄力和远见，让我顺利地完成了全部书稿。

谨以此书献给热爱 C 语言的朋友。

刘兴

中国，湖南

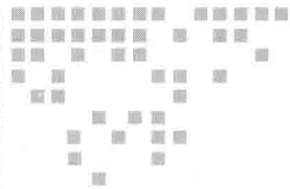
目　录 *Contents*

第一篇 Part 1

准 备 篇

我仍然爱着C语言。如此简单，如此强大。

——Java之父 詹姆斯·高斯林
（James Gosling）



Chapter 1 第 1 章

C 语言概述

C 语言是一种通用的、过程式的编程语言，其广泛应用于系统与应用软件的开发，具有高效、灵活、功能丰富、表达力强和可移植性强等特点，是最近 20 多年使用最为广泛的编程语言。C 语言是由美国的丹尼斯·里奇（Dennis M. Ritchie）于 1969 年至 1973 年以 B 语言为基础在贝尔实验室开发完成的。

1978 年之后，C 语言先后被移植到各种大、中、小型机及微型机上，它既可以作为工作系统设计语言编写系统应用程序，也可以作为应用程序设计语言编写不依赖计算机硬件的应用程序。目前，C 语言的编译器支持各种不同的操作系统，如 UNIX、Windows、Linux 等。C 语言的设计也在很大程度上影响了后来的编程语言，例如 C++、Objective-C、Java、C# 等。

1.1 C 语言的起源与发展

C 语言的发展历史颇为有趣，它的原型是 ALGOL 60。1963 年，剑桥大学将 ALGOL 60 发展成为 CPL（Combined Programming Language）；1967 年，剑桥大学的 Matin Richards 对 CPL 进行了简化，于是产生了 BCPL；1970 年，美国贝尔实验室的 Ken Thompson 对 BCPL 进行了修改，改名为 B 语言，同时用 B 语言编写了第一个 UNIX 操作系统；1973 年，美国贝尔实验室的丹尼斯·里奇在 B 语言的基础上最终设计出了一种新的语言，他选取 BCPL 的第二个字母作为这种语言的名字，即 C 语言，丹尼斯·里奇因此被世人称为“C 语言之父”。

为了推广 UNIX 操作系统，1977 年，丹尼斯·里奇发表了《可移植的 C 语言编译程

序》，1978 年，布莱恩·克尼汉（Brian W. Kernighian）和丹尼斯·里奇出版了名著《The C Programming Language》，使 C 语言迅速成为世界上流行最广的高级程序设计语言，K&R C 也因此确定了其事实性标准的历史地位。

随着微型计算机的日益普及，不同种 C 语言之间出现了不一致的问题，这一点为 C 语言的广泛应用带来了不便。1989 年，美国国家标准局（ANSI）颁布了第一个官方的 C 语言标准（X3.159-1989），简称 ANSI C 或 C89；1990 年，C89 被国际标准化组织（ISO）采用为国际标准（ISO/IEC9899:1990），简称为 C90，这是目前广泛使用并完全支持的标准。

1999 年，国际标准组织为 C 语言发布了新的标准 ISO/IEC 9899:1999，修正了 C89 标准中的一些细节，并增加了更多更广的国际字符集支持，这个标准通常被称为 C99，ANSI 于 2000 年 3 月采用 C99。

2011 年 12 月 8 日，ISO 正式发布了 C 语言的新标准 C11，之前被称为 C1X，官方名称为 ISO/IEC 9899:2011，新的标准提高了对 C++（1983 年由贝尔实验室的 Bjarne Stroustrup 推出，C++ 进一步扩充和完善了 C 语言，成为面向对象的程序设计语言）的兼容性，并增加了很多新的特性。

1.2 C 语言特性

2011 年 10 月 9 日，丹尼斯·里奇去世，享年 70 岁，Java 之父詹姆斯·高斯林（James Gosling）为此发表了纪念 C 语言之父丹尼斯·里奇的简短博文：“丹尼斯·里奇辞世的新闻如五雷轰顶，过去几天已经有很多资讯在报道此事，他的影响巨大，并超越了科技世界，虽然他的巨大影响可能不为人知，但完全可以感受到的是，C 语言撑起了一切。我的整个职业生涯也是从 C 语言和 UNIX 中发展而来的。”全世界的计算机爱好者都以他们特有的方式纪念这位编程语言的重要奠基人，很多人在众多的国际交互论坛中发帖悼念 C 语言之父，全帖仅仅只用一个分号“;”（在 C 语言中，分号标志着一行指令语句的结束）形象地表达了人们的怀念之情。

C 语言之父悄然离去，但 C 语言并没有因此衰退，近年来它仍然是世界主流的编程语言之一。在 2019 年 3 月的 TIOBE 编程语言排行榜中（如图 1-1 所示），C 语言仍处于第 2 位，并呈现上升势头。

C 语言主要有以下特性：

1）设计目标接近机器底层但不失跨平台性。C 语言提供了许多低级处理的功能，可搭配汇编语言来使用，著名的 C 编译器 GCC（UNIX 下常用的是 CC）保持着良好的跨平台的特性，以一个标准规格写出的 C 语言程序通过 GCC(或 CC) 可在许多计算机平台上进行编译，甚至包含嵌入式环境以及大型机平台。

2）C 语言编译生成的可执行文件短小精悍。C 语言能以简易的方式进行编译，可直接处理低级存储器，仅产生少量的机器码，并且不需要任何运行环境的支持便能运行。

3）C 语言虽简单但功能强大。C 语言仅有 32 个保留字符，使用传统的结构化设计，变量具有作用域、递归等优秀功能，编译预处理使得编译更具弹性，传递参数灵活，可采用值传递和指针传递两种方式，不同的变量类型可用结构体（struct）组合在一起；此外，C 指针很容易就能对存储器进行低级控制。

Mar 2019	Mar 2018	Change	Programming Language	Ratings	Change
1	1		Java	14.880%	-0.06%
2	2		C	13.305%	+0.55%
3	4	^	Python	8.262%	+2.39%
4	3	v	C++	8.126%	+1.67%
5	6	^	Visual Basic .NET	6.429%	+2.34%
6	5	v	C#	3.267%	-1.80%
7	8	^	JavaScript	2.426%	-1.49%
8	7	v	PHP	2.420%	-1.59%
9	10	^	SQL	1.926%	-0.76%
10	14	^^	Objective-C	1.681%	-0.09%

图 1-1　2019 年 3 月 TIOBE 编程语言排行榜

1.3　开发环境搭建

下面以“helloworld”C 程序（非 GUI 程序，运行在 Windows 的控制台和 UNIX/Linux 系统的终端）为例，讲解 Windows、类 UNIX/Linux 平台下的开发环境搭建（本书将以 UNIX/Linux 平台为主，对 C 指针及其应用进行讲解）。

1.3.1　Windows 开发环境

1. Microsoft Visual Studio

Microsoft Visual Studio（简称 VS）是美国微软公司的开发工具包系列产品。VS 是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具，如 UML 工具、代码管控工具、集成开发环境（IDE）等。所写的目标代码适用于微软支持的所有平台，包括 Microsoft Windows、Windows Mobile、Windows CE、.NET Framework、.NET Compact Framework、Microsoft Silverlight 及 Windows Phone。

微软公司提供了可供免费使用的 Visual Studio Community 2015（其具备所有为 Windows、iOS、Android 设备或是云服务器开发桌面、移动、网页应用的全套功能）。读者可通过 Microsoft 的网站下载 Visual Studio Community 2015（下载地址为：https://visuals-

tudio.microsoft.com/zh-hans/vs/older-downloads/)，加载ISO映射文件后再进行安装。安装完毕后再启动Visual Studio Community 2015，选择“Visual C++”项目中的“Win32控制台应用程序”(如图1-2所示)。

图1-2 Win32控制台应用程序建立

单击“确定”按钮，出现向导对话框，选中“附加选项”区域的“空项目”之后，单击“完成”按钮(如图1-3所示)。

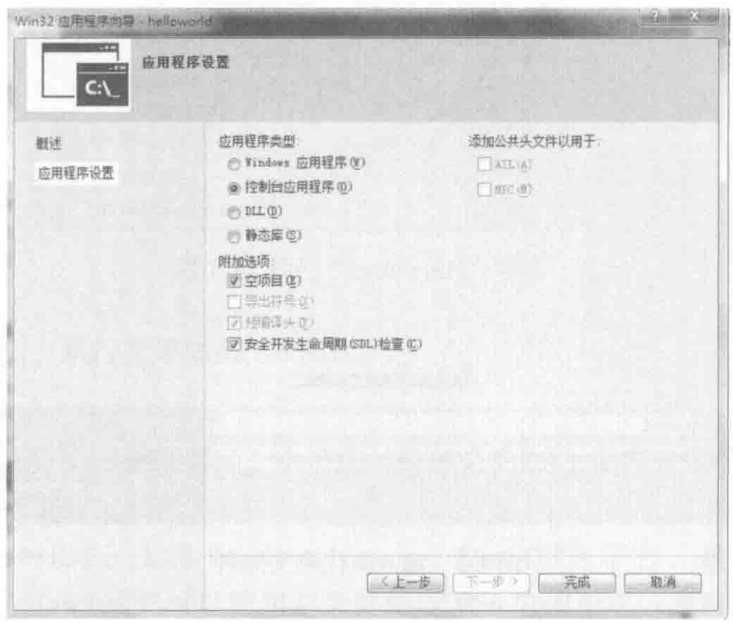


图1-3 Win32应用程序向导

由于刚才建立项目时选择了“空项目”，因此需要增加 C 源代码文件，在源文件处点击鼠标右键，选择“添加”→“新建项”（如图 1-4 所示），输入源代码文件名“main.c”（如图 1-5 所示）。

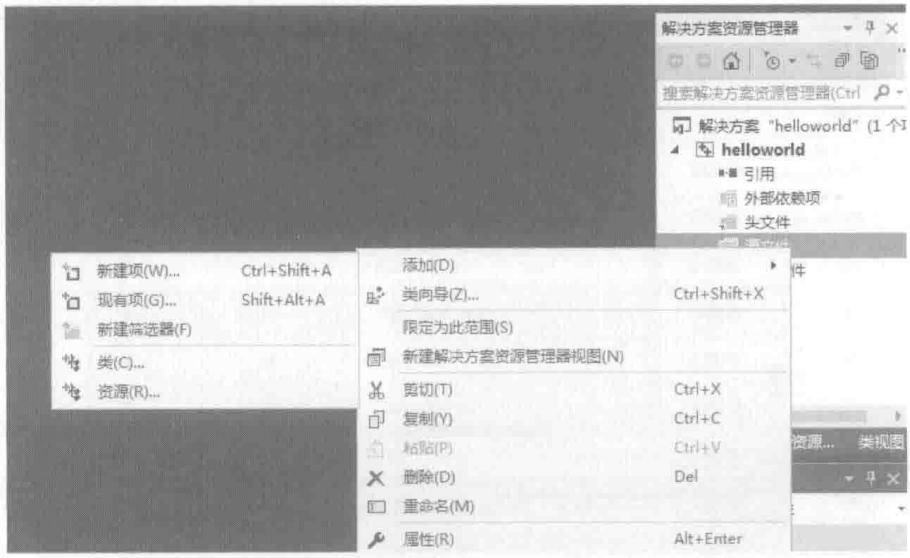


图 1-4 增加 C 源代码文件

图 1-5 输入源代码文件名

在屏幕的左边输入“helloworld”的 C 语言代码（如图 1-6 所示）。

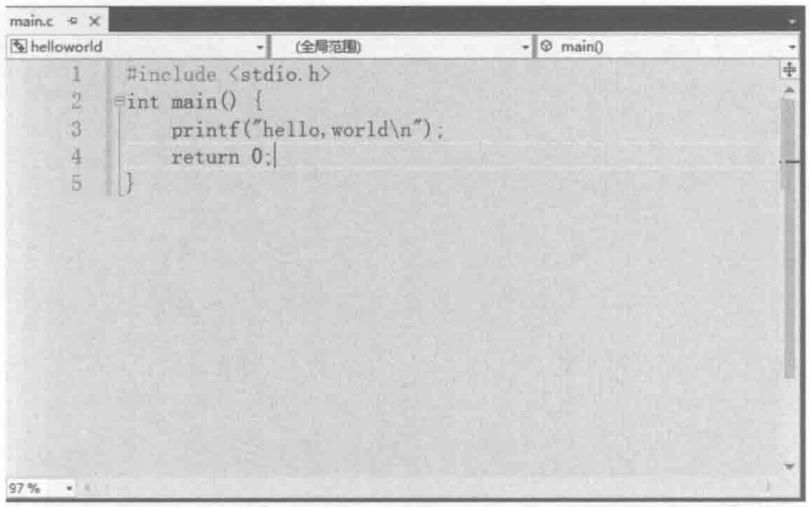


图 1-6 “helloworld”C 语言源代码

选择“调试”菜单的“开始执行”(如图 1-7 所示)。

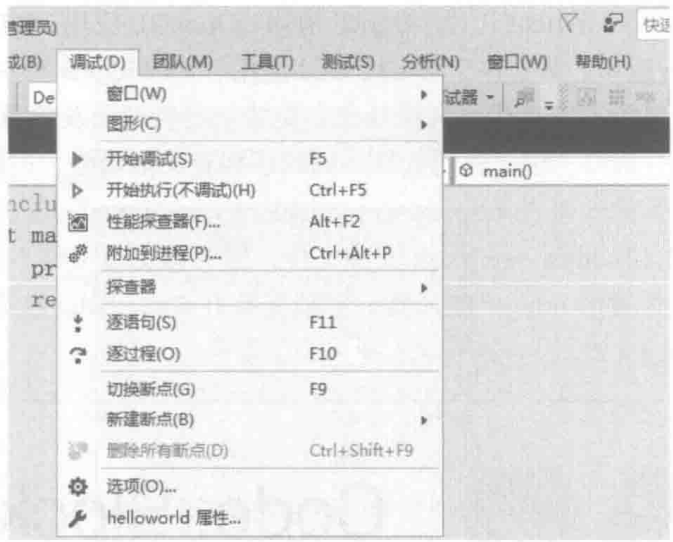


图 1-7 执行“helloworld”程序

程序经过编译后，执行效果如图 1-8 所示。

2. Code::Blocks

Code::Blocks 是一个开放源码的、全功能的跨平台 C/C++ 集成开发环境，它由 C++ 语言开发完成，使用了著名的图形界面库 wxWidgets。相比 Visual Studio 而言，Code::Blocks 是跨越平台的 C/C++IDE，支持 Windows、Linux、Mac OS X 平台，最重要的是它遵守 GPL 开源协议，Windows 用户可以使用它免费编译 Win 应用程序以及跨平台的应用程序，而无须依赖于 Visual Studio。

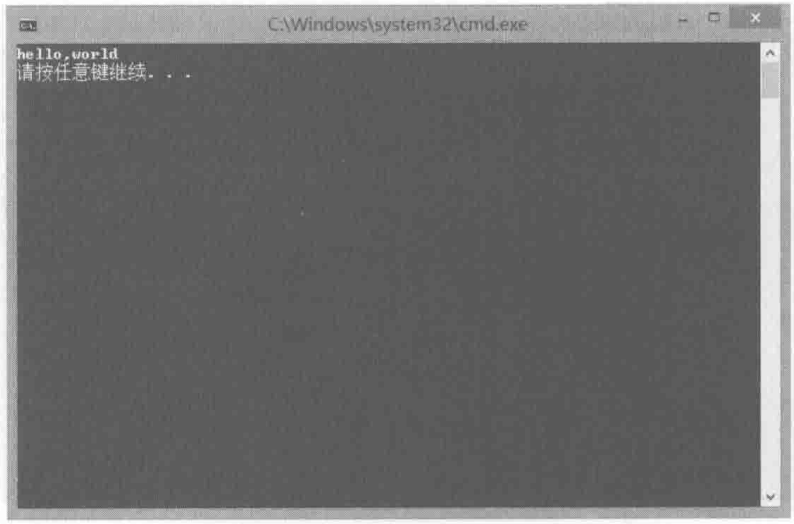


图 1-8 “helloworld”程序执行效果

Code::Blocks 提供了许多工程模板，包括控制台应用、DirectX 应用、动态链接库、FLTK 应用、GLFW 应用、Irrlicht 工程、OGRE 应用、OpenGL 应用、QT 应用、SDCC 应用、SDL 应用、SmartWin 应用、静态库、Win32 GUI 应用、wxWidgets 应用、wxSmith 工程等；它支持语法彩色醒目显示，支持代码自动补全，支持工程管理以及项目构建、调试；此外，它还支持插件、代码分析器、编译器的选择，同时还拥有灵活而强大的配置功能。

Code::Blocks 的下载地址为 http://www.codeblocks.org/downloads，Windows 平台下建议下载 codeblocks-13.12mingw-setup.exe 安装文件，因为该安装文件不仅包括 Code::Blocks 本身，还将含有开源免费的 mingw 编译器。下载安装好 Code::Blocks 之后，启动它，启动过程中会显示它的 logo（如图 1-9 所示）。

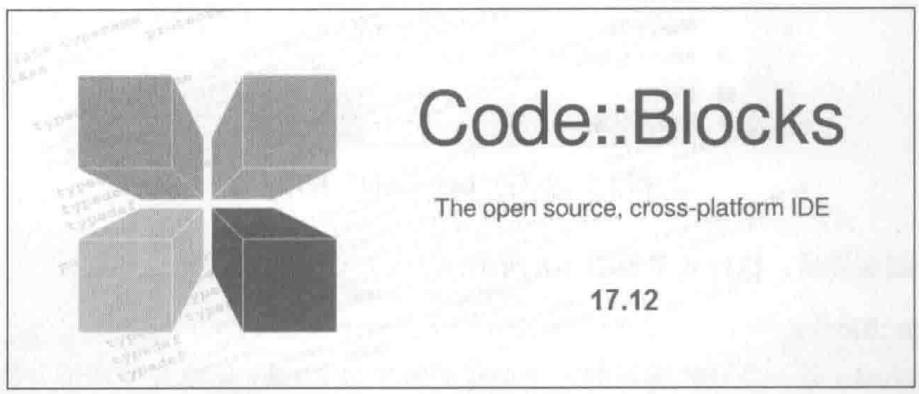


图 1-9 Code::Blocks 启动界面

启动 Code::Blocks 之后，选择“New”→“Project”，新建项目（如图 1-10 所示）。在项目模板中选择“Console application”（控制台程序），如图 1-11 所示。