有限域上基于 Gröbner 基的高级综合优化方法

王冠军[1]，赵 莹[1]，王茂励[2]

（1. 中国矿业大学 计算机科学与技术学院，江苏 徐州，221116，zywgj@cumt.edu.cn；2. 山东省计算中心，济南 250014）

摘 要：提出了基于多项式符号代数的高级综合方法，并使用元件库中的元件构建多项式符号代数所表示的数据通路，计算出其 Gröbner 基. 利用 Gröbner 基对多项式进行一些基本操作，例如，多变元多项式分解、最大公因式提取、库单元映射等，从而实现了有限域上的数据通路优化. 最后进行了算法复杂性分析和实验，实验在 SUN 工作站上通过调用 Maple10 来完成，实验结果证实了本方法的有效性.

关键词：高级综合；多项式符号代数；Gröbner 基；有限域

中图分类号：TN401 **文献标志码**：A **文章编号**：0367－6234(2010)07－1153－05

High level synthesis optimization approach based on Gröbner basis over finite field

WANG Guan-jun[1], ZHAO Ying[1], WANG Mao-li[2]

(1. School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China, zywgj@cumt.edu.cn; 2. ShanDong Computer Science Center, Jinan 250014, China)

Abstract: The high level synthesis approach based on PSA is proposed. The datapath represented by PSA was constructed with the library elements firstly, then the basis of polynomial representation datapath was computed. Some operations were implemented using basis, such as multivariate polynomial decomposition, the greatest common divisor extraction, library mapping and so on, thus the optimization of datapath with these operations was achieved. The complexity analysis of algorithm was carried out. The experiment was implemented on the SUN station with Maple10. The results show the efficiency our method.

Key words: high level synthesis; polynomial symbolic algebra (PSA); basis; finite field

根据美国半导体协会制订的 2005 年国际半导体技术发展路线及其在 2006 年的更新，未来 15 年集成电路仍将按摩尔定律持续快速发展. 预计到 2010 年，高性能 CPU 芯片上可集成的晶体管数目将超过 20 亿个（到2018 年超过 140 亿个），片上局部时钟频率可达到 15 GHz（到 2018 年超过 53 GHz），Intel 总裁 Craig Barrett 预测说，传统的芯片制造技术有可能支撑到 5 nm 的范围[1]. 半导体技术的这些进步，使单个芯片上集成更复杂和更灵活的系统成为可能. 半导体技术的迅猛发展的主要原因是：1）需求牵引；2）技术驱动. 这也促使芯片的设计技术在越来越高的层次上进行，高级综合应运而生，各种综合的方法和优化技术也不断出现. 本文是在电路的多项式符号代数表示基础上，在有限域上通过多项式的各种运算，进行综合优化. Gröbner[2] 基主要用来做理想成员判定和代数方程求解，在本文中主要用于域上多项式分解和多项式最大公因式（GCD）的计算方面，在库单元映射方面也有重要应用.

收稿日期：2008－10－23.

基金项目：国家自然科学基金资助项目（69973014）；中国矿业大学青年科研基金资助项目（2009A051）.

作者简介：王冠军（1981—），男，博士，讲师.

1 有限域代数与 Gröbner 基

1.1 有限域代数

以素数 P 为模的整数剩余类环构成 P 阶有限域 $GF(P)$. 在任何 P 阶有限域中能找到一个生成元素 a，它能生成域中所有 $P-1$ 个非 0 元素，从而构

成一个循环乘群 $G(a):1,a,a^2,\cdots,a^{p-2},a^{p-1}=1$. 域中非 0 元素所构成的乘法群之阶定义为域中该元素的级. 有限域的元素个数是素数. 可以定义两类有限域,$GF(P)$ 和它 m 度的扩展 $GF(P^m)$. 基本域 $GF(P)$ 中包含元素 $\{0,1,2,\cdots,p-1\}$, 最小的域是 $GF(2)$. 它的加法操作相当于电路异或操作而乘法操作则相当于与操作.

定义 1(多项式环) 假定 F 为有限域,域上以 x 为变元的多项式为

$$\alpha_0+\alpha_1 x+\alpha_2 x^2+\cdots\alpha_k x^k=\sum_k \alpha_i x^i.$$

式中:$\forall \alpha_i \in F$,α_i 为系数,k 为阶. α_k 称为首项系数,如果 $\alpha_k=1$,则称多项式为首一多项式,域上所有以 x 为变元的多项式组成一个多项式环 $F[x]$. 相似的定义 $F[x_1,x_2,\cdots,x_d]=A$,表示域上 d 个变元的多项式环. 当 $F=GF(2^m)$ 时,相应的多项式则以 2^m 为模.

1.2 Gröbner 基

域 k 上的关于 $x_1,\cdots,x_n$ 的全体多元多项式的集合记为 $k[x_1,\cdots,x_n]$,容易验证 $k[x_1,\cdots,x_n]$ 对于多元多项式的加法与乘法运算构成一个含有单位元的交换环,称之为多项式环.

定义 2 设 $F=\{f_1,\cdots,f_l\}$ 为一个多元多项式集合. 由 F 生成的理想记为 $I=<F>$:

$$\langle F\rangle=\{h_1f_1+\cdots+h_lf_l \mid h_1,\cdots,h_l\in k[x_1,\cdots,x_n]\}.$$

多项式 $F=\{f_1,\cdots,f_l\}$ 称为生成该理想的基,由于 F 是有限的,故称该理想是有限生成的. Hilbert 基理论证明了任何一个理想都是有限生成的.

定义 3 给定了 N^n 上的一个可容许的排序 $>$,设 $f\in k[x_1,\cdots,x_n]$,定义为

1) f 的 multidegree 为

$\text{multideg}(f)=\max(\alpha\in N^n:a_\alpha\neq 0)$.

2) f 的首项单项式为

$LM(f)=X^{\text{multideg}(f)}$.

3) f 的首项系数为

$LC(f)=a_{\text{multideg}(f)}$.

4) f 的首项为

$LT(f)=LM(f)LC(f)$.

定义 4 设多项式 $r\in k[x_1,\cdots,x_n]$,$F=\{f_1,\cdots,f_s\}\subseteq k[x_1,\cdots,x_n]-\{0\}$ 为环 $k[x_1,\cdots,x_n]$ 中零多项式的有限集合. 若 $r=0$ 或者 r 模 F 不能约化,即 $LT(f_i)$,$i=1,2,\cdots,s$,中任一项都不是 r 中所出现的各项的因子,则称多项式 r 对 F 是既约的,记为 $f\xrightarrow{F}{}^{*} r$. 进而,若 $f\xrightarrow{F}{}^{*} r$,则称 r 为 f 相对 F 的余多项式.

定义 5 设 I 是环 $k[x_1,\cdots,x_n]$ 上的一个非零理想,$G=\{g_1,\cdots,g_s\}$ 是 I 中非零多项式的有限集合,称 G 是理想 I 的 Gröbner 基,当且仅当对于 I 中的每个非零多项式 f,存在 $g_i\in G$ 使得 $LT(g_i)\mid LT(f)$.

定义 6 设 $f,g\in k[x_1,\cdots,x_n]-\{0\}$,$L=lcm(LM(f),LM(g))$. 其中,$lcm$ 为最小公倍式. 令 $S(f,g)=\frac{L}{LT(f)}f-\frac{L}{LT(g)}g$. 称多项式 $S(f,g)$ 为 f 和 g 的 S - 多项式.

定义 7 称环 $k[x_1,\cdots,x_n]$ 中的 Gröbner 基 $G=\{g_1,\cdots,g_s\}$ 是既约的,用 RGB 表示,若对于所有的 i,$1\leqslant i\leqslant s$ 为:

1) $LC(g_i)=1$.

2) g_i 相对于 $G-\{g_i\}$ 是既约的,即 g_i 中没有非零项可以被任何 $LM(g_j)$,$j\neq i$,除.

可以证明一个理想的既约 Gröbner 基唯一.

2 有限域上高级综合优化

将 Gröbner 基理论应用到了数据通路的综合中. $L=\{l \mid l$ 为元件库中元件的多项式表示$\}$. 为了使用元件库中的元件构建多项式 s 所表示的数据通路,一个必要条件是:$s\in <L>$. 为了检验 s 是否为 $<L>$ 中的元素,首先需要计算出 $<L>$ 的 Gröbner 基 G,然后执行除法算法 Reduce(s, G),设 $s=\sum_i u_ig_i+r$. 若 $r=0$,则 s 为 $<L>$ 中的元素;更进一步,若 $\forall i,u_i,g_i\in L$,则该数据通路可以用元件库中的元件来构建.

综合算法中同时引入了高层次重构技术和对多项式的一些基本操作(加/减、乘法、除法、倒置等)及传统的算术电路设计中的代数变换技术,例如词 - 重写技术[3]、因式分解[4]、树高度缩减[5]、Horner 形式与提取公因式[6]、系数的模块与分段、分解与扩展、代数冗余消除等,从而实现了基于最少器件数、最小时延等不同目标的数据通路优化. 优化的目标是产生表示不同但功能相等的结果.

2.1 多变元多项式分解

目前不少符号计算软件都提供因式分解的函数完成多元多项式的分解这种计算. 本文将 GOPALAKRISHNAN[7] RTL 级缩减算法改造应用在行为级分解中,并给出有限域上的多变元多项式分解算法.

1) 待分解多项式 f,有限域 $F(2^m)$;

2) $x_1,x_2,\cdots,x_d$ 为多项式中 d 个变元;

3) $SF(n)=k$ 为 n 整除 $k!(n\mid k!)$;

4) $Y_{k(x)} = x(x-1)\cdots(x-k+1)$ 称为降阶乘积方程;

5) $Y_k = \prod_{i=1}^{d} Y_{k_1}(x_1) Y_{k_2}(x_2)\cdots Y_{k_d}(x_d)$ 称为降阶乘积方程在多变元多项式中推广;

6) μ_i 定义为:$\mu_i = \min\{2^{n_i}, SF(2^m)\}$;$i = 1, 2, \cdots, d$.

域上多变元多项式分解算法的程序为:

Reduce (f, d, x, m)

输入:$f \in k[x_1, \cdots, x_n]$,

$F = \{f_1, \cdots, f_s\} \subseteq k[x_1, \cdots, x_n] - \{0\}$

项序 $>$

其中,r 相对于 F 是即约的.

输出:$r, u_1, \cdots, u_s \in k[x_1, \cdots, x_n]$,使得

$$f = \sum_{i=1}^{s} u_i f_i + r$$

1. 计算 $SF(2^m)$

for $i = 1$ to d do

2. $\mu_i = \min\{2^{n_i}, SF(2^m)\}$;

/ * * $k[i]$ 为多项式中 $x[i]$ 的最大度数 * * /

3. end for

/ * * 初始值计算 * * /

4. for $i = 1$ to d do

5. if $k[i] \geqslant \mu[i]$ then

6. $quo, rem = \dfrac{f}{Y_{<0,\cdots k[i],\cdots 0>}(x_1, \cdots, x_d)}$

7. if$(rem = = 0)$ then

8. $r = 0$ return;

9. else $f = rem = r$; $f_i = quo$,

$\mu_i = Y_{<0,\cdots k[i],\cdots 0>}(x_1, \cdots x_d)$

10. break;

11. endif

12. endif

13. end for

/ * * 初始循环判定 f 是否整除,否则继续进行下阶段分解 * * /

14. for $j = \prod_{l=1}^{d} \mu_l$ to 1 *do*

15. for $i = 1$ to d do

16. $k[i] = x[i]$

/ * * 在多项式 f 单项式排序中的次大阶中度数 * * /

17. end for

18. $quo, rem = \dfrac{f}{Y_{<k[0],\cdots,k[d]>}(x_1, \cdots, x_d)}$

19. $b_{<k[0],\cdots,k[d]>} = \dfrac{2^m}{\gcd\left(2^m, \prod_{i=1}^{d} k[i]!\right)}$

20. if $b_{<k[0],\cdots,k[d]>} \mid quo$ then

21. if $(rem = = 0)$ then

22. return

23. else

24. $f = rem = r$　$f_i = quo$,

$\mu_i = Y_{<0,\cdots k[i],\cdots 0>}(x_1, \cdots, x_d)$

25. endif

26. endif

27. $c_k = < k[0], \cdots, k[d] >$ 的系数

28. if $c_k > b_{<k[0],\cdots,k[d]>}$

29. $quo, rem = \dfrac{f}{b_{<k[0],\cdots,k[d]>} Y_{<k[0],\cdots,k[d]>}(x_1, \cdots, x_d)}$

30. $f = rem = r$　$f_i = quo$,

$\mu_i = b_{<k[0],\cdots,k[d]>} Y_{<k[0],\cdots,k[d]>}(x_1, \cdots, x_d)$

31. endif

32. end for

33. return $f = \sum_{i=1}^{s} u_i f_i + r$

算法核心思想是将多元问题转化为一元问题来解决. 算法首先计算 $SF(2^m)$,然后利用它计算 μ_i 值. 找出多项式每个变量的最大度数 k_i,利用 Y_{u_i} 分解多项式,将余数作为新的多项式,重新计算 k_i 和 Y_{u_i}, $Y_{u_i} \sim Y_0$ 循环分解. 分解后,进行判断:

1) 如果 quo 可以为两多项式相乘形式,且余数为 0,结束;

2) 如果 quo 可以为两多项式相乘形式,且余数为不为 0,将余数作为新多项式继续分解;

3) 如果系数 $c_k > b_k$,将除数定义为 $b_k \cdot Y_k$,将余数作为新多项式继续分解.

算法可在 Maple 中实现且复杂度为 $O(\prod_d \mu_i)$,在实际的电路分解中,可依据不同的优化目标进行针对性的分解,例如,于最小元器件的分解,基于最低功耗的分解等.

2.2　有限域上基于既约 Gröbner 基的 GCD 计算

Gröbner 基应用广泛,既约 Gröbner 基在有限域上针对多项式符号代数表示电路在最大公因子提取方面的应用. 最大公因子(GCD)提取是多项式分解等操作的基础,其中给出几个相关性的定义为:$A = k[x_1, x_2, \cdots, x_n]$ 为域 k 上 n 变元多项式环.

定义 8(消元序)　设 X_1 和 X_2 是变元 x 的幂积,Y_1 和 Y_2 是变元 y 的幂积. 定义为

$$X_1 Y_1 < X_2 Y_2 \Leftrightarrow \begin{cases} X_1 <_x X_2, \\ X_1 = X_2 \text{ 和 } Y_1 <_y Y_2. \end{cases}$$

容易验证,定义的序 $<$ 是项序,则称这个项序为 x 变元大于 y 变元的消元序.

定理 1(消元定理) 令 I 是域 k 上环 $k[y_1,\cdots,y_m,x_1,\cdots,x_n]$ 中的非零理想,项序 $<$ 是 x 变元大于 y 变元的消元序,令 $G=\{g_1,\cdots,g_t\}$ 是理想 I 的 Gröbner 基,则 $G\cap k[y_1,\cdots,y_m]$ 是理想 $I\cap k[y_1,\cdots,y_m]$ 的基.

由于有限域上的多项式环 $A=k[x_1,x_2,\cdots,x_n]$ 是唯一因子分解整环,该环中的任何2个多项式都有最大公因子. 但是,环 $k[x_1,x_2,\cdots,x_n],n\geqslant 2$,不是主理想环,更没有欧几里得除法算法,因此要计算最大公因子非常困难,本文应用消元理论解决,给出算法 GCD-RGB 为:

步骤 1 假设 $f,g\in k[x_1,x_2,\cdots,x_n]$.

步骤 2 令 $d=\gcd(f,g)$ 为 f,g 的最大公因子($lc(d)=1$),d 由 f 和唯一确定.

步骤 3 计算 $l=lcm(f,g)$ 为 f,g 的最小公倍,其中,$lc(l)=lc(f).lc(g)$.

步骤 4 得到 $f.g=lcm(f,g)\gcd(f,g)<lcm(f,g)>=<f>\cap<g>$.

步骤 5 得到 $\gcd(f,g)=\dfrac{fg}{lcm(g,f)}$.

步骤6 在环 $k[x_1,x_2,\cdots,x_n,\omega]$ 中相对 x 变元小于 ω 变元的消元序计算理想 $<\omega f,(1-\omega)g>$ 的既约 Gröbner 基 G,再求 $G\cap k[x_1,x_2,\cdots,x_n]$. 由于 $G\cap k[x_1,x_2,\cdots,x_n]=\{lcm(f,g)\}$,即 $lcm(f,g)$ 就是 G 中 ω 变元不出现的那个多项式. 由于 G 是 $<f>\cap<g>$ 的既约 Gröbner 基,用除法算法可得到 h,使得 $fg=h.lcm(f.g)$,于是计算出 $\gcd(f,g)=h$.

2.3 库单元映射

现代高层次设计的输出常常需要映射到组件库中,在这种情况下,库单元映射成为支撑高层次设计的有效手段. 在本文中库单元映射的输入为数据通路的多项式表示和库单元的多项式表示,输出则为数据电路全部映射为库单元中的基本电路模块. 给出库单元映射方法为:

输入:数据通路的多项式表示

库单元的多项式表示

输出:电路模块是否可映射

BEGIN

while(the input is not empty)

{compute the characteristic polynomial of the input $<f_i>$ and $<L>$

Compute the Gröbner basis $<G>$ of the library element set $<L>$

For(every $i\leqslant k$)

If ($<f_i>\in<G>$)

Then return(yes)

else

return(no)

}

END

算法中假设数据通路可分解为 k 个多项式,通过以上算法就可以判定给定数据通路多项式是否可映射,首先计算待替换数据路径中电路的特征多项式,然后从元件库中寻找基本电路模块并计算其 Gröbner 基,最后进行比较判断,如果所有的多项式模块都可映射为元件库中单元,那么就可以进行替换的工作. 库单元映射通常有基于最少元件数映射和基于最小关键路径延迟映射等方法. 本文给出考虑多目标约束的映射方法,方法基于整数线性规划(ILP)模型,每个数据通路多项式可以由一个或多个库单元构成,其目标函数为

$$\text{minMapping}_{(\text{component},\text{area},\text{CPD},\text{PDP})}.$$

式中:约束条件分别为组件数,面积,关键路径延迟(CPD)和功耗时延积(PDP). 给出一组映射如图 1 所示.

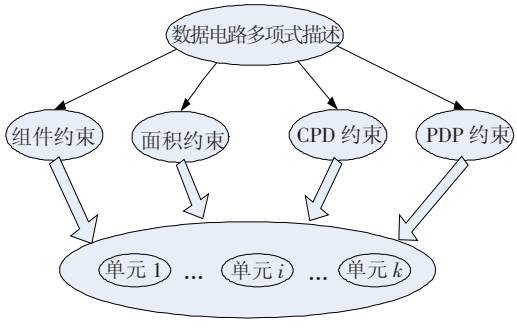

图 1 基于多目标约束的库单元映射

当目标函数和各约束条件生成之后,就可以利用成熟的 ILP 工具来解决,使用 ILP 交集解法并最终得到映射方案. 这种方法简单易行,时间复杂度亦在可以允许的范围内,因此是有效的.

3 实验验证

多项式表达式出现在许多现实的应用中,例如数字信号处理和3D 图形图像领域. 为便于比较,实验环境设置如文献[7]中所示,输入多项式的综合只用加法器与乘法器来构建完成. 应用 Synopsys Design compiler 工具(时钟周期 40 ns,工作电压 5 V,1.0 μ power2_sample.db 技术库)估计加法器和乘法器的面积和延时. 面积和延时的估计结果如表 1所示,其中的加法器和乘法器均为 16 bit. 实验中用到的多项式集合如表 2 所示,本实验选取了 7 个多变元多项式,多项式因式分解的结果如表 3 所示,其中,CPD 为电路中关键路径延时.

表 1　库单元的延迟和面积

库单元	延迟/ns	面积/mm²
加法器	177	10.24
乘法器	3 140	18.56

表 2　多项式实验电路

电路名称	电路表达式
P1	$a^2 - b^2$
P2	$b^3 + ba^2c$
P3	$1 - \frac{1}{2}x^2 + \frac{1}{24}x^4 + x + yz$
P4	Gabor-Tranform(多用于神经网络)
P5	$ac + ad + bc + bd + b^2d^2$
P6	$a^2 + 2ab + b^2 + x^2 + 2xy + y^2 + 1$
P7	$ax + ay + a + x + y + 1$

表 3　多项式分解的综合实验结果

实验电路	未分解前		分解后		改进度/%	
	面积	CPD	面积	CPD	面积	CPD
P1	4 798	27.31	3 501	29.80	27.03	-9.11
P2	13 940	41.30	10 490	29.90	24.75	27.60
P3	7 269	85.88	6 789	56.30	6.47	34.44
P4	47 833	106.22	24 213	85.44	49.38	19.56
P5	21 831	41.40	12 472	63.07	42.87	-52.34
P6	15 957	31.80	6 425	42.32	59.74	-33.08
P7	6 830	29.74	3 197	35.10	53.20	-18.02
平均					37.63	-4.36

从表 3 的实验综合结果来看，域上多项式分解可以有效的降低芯片面积（平均减少 37.63%），但与此同时会带来 CPD 的少许增加（平均增加 4.42%），这是因为多项式的分解会使一个较大的多项式变为几个小的多项式，减少了优化延迟的机会，因此使 CPD 出现了少许增加，要解决这个问题，可以通过增加代价函数的方法来进行折衷.

库单元映射方法本文选取了一些典型的实验电路，在各种约束下得到的映射结果如表 4 所示，从采用基于 ILP 模型的交集解法得到映射结果来看，最高的改进达到 23.3%，平均改进达到 14.6%.

表 4　典型电路的库单元映射结果　%

电路名称	组件约束	面积约束	CPD 约束	PDP 约束	基于 ILP 方法
Gabor-Transform	14.2	9.5	15.0	16.2	13.1
Hufman	23.2	14.2	12.2	16.7	17.2
PSK	17.8	11.2	17.6	21.1	15.4
IDCT	14.2	6.8	10.3	4.9	10.1
Anti-alias	22.2	28.9	31.1	19.2	23.3
Sub Band	7.8	11.2	16.4	18.4	11.1
Dequent	10.2	8.8	15.1	14.4	12.1

4　结　论

1）文献[8－10]给出了多项式优化的一些最新的研究成果，这也表明了多项式符号代数的生命力，在此基础上的有限域多项式优化仍将是一个较新的研究方向.

2）由于多项式规模对 Gröbner 基的计算有重要影响，因此在优化过程中需要考虑计算复杂度问题.

参考文献：

[1] 安虹. 用可重构计算技术实现高效能通用微处理芯片[J]. 信息技术快报，2006，4(6)：11－34.

[2] BUCHBERGER B. An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-dimensional Polynomial Ideal(in German)[D]. Austria：University of Innsbruck，1965.

[3] ARVIND，SHEN X W. Using term rewriting systems to design and verify processors[J]. IEEE Micro，1999，19(3)：36－46.

[4] HOSANGADI A，KASTNER R，FALLAH F. Energy efficient hardware synthesis of polynomial expressions[C]//Proceedings of the 18th International Conference on VLSI Design held jointly with 4th International Conference on Embedded Systems Design. Washington：IEEE Computer Society，2005：653－658.

[5] MANGALAM G N，NARAYAN S，van BESOUW P，Avra. Graph transformations for improved tree height reduction[C]//Proceedings of the 16th International Conference on VLSI Design. Washington：IEEE Computer Society，2003：474－479.

[6] HOSANGADI A，FALLAH F，KASTNER R. Optimizing polynomial expressions by algebraic factorization and common subexpression elimination[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems，2006，25(10)：2012－2022.

[7] JABIR A M，PRADHAN D K，MATHEW J. An Efficient technique for synthesis and optimization of polynomials in GF(2^m)[C]//Proceedings of the 2006 IEEE/ACM international conference on Computer-aided design. New York：ACM，2006：151－157.

[8] XING Xianwu，JONG ChingChuen. Using symbolic computer algebra for subexpression factorization and subexpression decomposition in high level synthesis[C]//Proceedings of the IEEE International Symposium on Circuits and Systems(ISCAS). Japan：IEEE，2005：5645－5648.

[9] WANG Jian，JIANG Anping. An area-efficient design for modular inversion in $GF(2^m)$[C]//Proceddings of the IEEE Asia Pacific Conference on Circuits and Systems(APCCAS). Singapore：IEEE，2006：1496－1499.

[10] JING M H，CHEN J H，CHEN Z H，*et al*. Low complexity architecture for multiplier inversion in $GF(2^m)$[C]//Proceddings of the IEEE Asia Pacific Conference on Circuits and Systems(APCCAS). Singapore：IEEE，2006：1492－1495.

（编辑　张　红）