

文章编号: 2095-4980(2019)06-1112-06

混合 RM-DRM 逻辑及其在可逆电路综合中的应用

卜登立

(井冈山大学 电子与信息工程学院, 江西 吉安 343009)

摘要: 为获得布尔函数的紧凑逻辑表示, 进而改善综合所得电路的质量, 提出一种混合 Reed-Muller 和对偶 Reed-Muller(RM-DRM)逻辑模型。基于海明距离对立方体集合进行划分来构建函数的混合 RM-DRM 逻辑表示, 并利用对偶原理借助 EXORCISM-4 工具对混合 RM-DRM 逻辑进行化简。最后将混合 RM-DRM 逻辑作为结构表示模型应用于可逆电路综合。实验结果表明, 与采用 RM 逻辑作为表示模型相比, 混合 RM-DRM 逻辑模型的采用可以降低某些函数综合所得可逆电路的量子成本, 并且能够降低 RevLib 库中的 134 个函数综合所得可逆电路的平均量子成本。

关键词: Reed-Muller 逻辑; 对偶 Reed-Muller 逻辑; 对偶原理; 可逆电路

中图分类号: TN02; TP391.72 **文献标志码:** A **doi:** 10.11805/TKYDA201906.1112

Mixed RM-DRM logic and its application in reversible circuit synthesis

BU Dengli

(School of Electronics and Information Engineering, Jinggangshan University, Ji'an Jiangxi 343009, China)

Abstract: A mixed Reed-Muller and Dual Reed-Muller(RM-DRM) logic model is proposed to achieve a more compact logic representation for a Boolean function and improve the quality of the synthesized circuit. The mixed RM-DRM logic representation for a Boolean function is constructed by using Hamming distance based cube cover partitioning, and is optimized by using EXORCISM-4 tool on the basis of duality principle. Being used as a structural representation model, the mixed RM-DRM logic is applied to reversible circuit synthesis. The experimental results show that compared to the Reed-Muller logic model, the mixed RM-DRM logic model can reduce the quantum cost of the synthesized reversible circuits for some functions, and can reduce the average quantum cost of the synthesized reversible circuits for the 134 functions from RevLib benchmark suite.

Keywords: Reed-Muller logic; Dual Reed-Muller logic; duality principle; reversible circuit

Reed-Muller(RM)逻辑是由异或运算连接一组乘积项的逻辑表示, 与由或运算连接一组乘积项的逻辑表示相比, 对于算术、校验以及通信等电路具有面积上的优势, 并能够实现具有通用测试集的可测试性电路设计^[1]。近年来 RM 逻辑也在信息安全领域的电路, 如 AES 加密电路中的 S 盒电路^[2]、基于 FinFET 的安全绝热电路^[3]等设计中得到了实际应用。可逆计算是信息无损的计算模式, 在纳米技术、光计算、极低功耗电路设计等新兴技术领域有着重要应用^[4]。由于门运算的固有可逆性, 可逆逻辑成为量子计算机的基本组成形式以及量子电路模型的核心部分^[5], 可逆电路综合也被视为量子电路综合中的一个必要阶段^[6]。异或运算是可逆计算和量子计算的基本构件, 特别是 RM 逻辑的乘积项可以直接映射为混合极性多控制 Toffoli(Mixed-Polarity Multiple-Control Toffoli, MPMCT)门, 因此, RM 逻辑作为结构表示模型^[7]在可逆电路以及量子电路的综合与设计也得到了应用^[6-7]。文献[8]研究了 RM 逻辑与布尔量子运算之间的直接对应关系, 并将量子电路表示为 RM 展开形式, 随后文献[9]使用 RM 逻辑最一般化的表示形式一积之异或和(Exclusive-Sum-Of-Products, ESOP)展开作为结构表示模型进行可逆电路的综合。可逆电路所实现的函数必须是双射, 并且可逆电路中不允许直接使用扇出或反馈^[10], 在进行可逆电路综合时应该遵循这些限制。从可逆电路综合方法所采用的函数表示模型来看, 除基于 RM 逻辑模型的综合方法外, 还有基于轮换^[11]、基于真值表^[12]以及基于决策图^[4,13]的综合方法。与基于群

收稿日期: 2018-09-11; 修回日期: 2019-03-27

基金项目: 国家自然科学基金资助项目(61961203,61640412); 江西省教育厅科技计划项目资助项目(GJJ160746); 井冈山大学博士科研启动项目资助项目(JZB1803)

论和基于真值表的综合方法相比，基于 RM 逻辑模型的可逆电路综合方法具有两个方面的优势，一是由于 RM 逻辑表示模型比较紧凑，能够处理较大规模的函数，因此具有较好的可扩展性；二是无需事先将不可逆函数嵌入到可逆函数^[7]，因此具有相对较高的时间效率，因为将不可逆函数嵌入到可逆函数的最优嵌入问题是 coNP 难^[14]问题。与基于决策图的综合方法相比，使用 RM 逻辑作为结构表示模型进行可逆电路综合所得电路虽然具有较高的量子成本，但所需的量子位硬件资源相对较少，因为对于一个 n 输入 m 输出的函数，基于 RM 逻辑模型的可逆电路综合方法使用 $n+m$ 条线来综合可逆电路^[9]，因此量子位数也为 $n+m$ ，而基于决策图的可逆电路综合方法却因决策图中结点的广泛共享导致了大量辅助线的采用，使得某些函数综合所得可逆电路的量子位数要远远大于 $n+m$ 。

对偶 RM(DRM)逻辑是 RM 逻辑的对偶表示形式，对于不同的函数，其 RM 逻辑表示与 DRM 逻辑表示可能具有不同的复杂度，这导致由这两种逻辑表示综合所得电路的成本也有所不同^[15]。如果将一个函数同时采用 RM 逻辑与 DRM 逻辑进行表示，则有可能获得成本较低的电路。本文提出用于表示布尔函数的混合 RM-DRM 逻辑模型，介绍了混合 RM-DRM 逻辑的构建与化简方法。将混合 RM-DRM 逻辑作为结构表示模型应用于可逆电路综合，给出了基于混合 RM-DRM 逻辑模型的可逆电路综合方法，并使用 RevLib 库中的函数^[16]对综合方法进行了验证。

1 混合 RM-DRM 逻辑及其化简

1.1 混合 RM-DRM 逻辑模型

对于具有 n 个输入变量 $\{x_i | 1 \leq i \leq n\}$ 、 m 个输出变量 $\{f_j | 1 \leq j \leq m\}$ 的布尔函数 F ，其 RM 逻辑表达式为：

$$F(x_1, x_2, \dots, x_n) = \bigoplus_{u=1}^t B_u T_u \quad (1)$$

式中： $F = [f_1, f_2, \dots, f_m]^T$ ；“ \oplus ”表示异或运算； $T_u = \bigwedge_{i=1}^n \hat{x}_i$ 为乘积项， $\hat{x}_i \in \{-, \bar{x}_i, x_i\}$ ，如果 $\hat{x}_i \neq -$ ，则称其为 T_u 中的一个文字； t 为乘积项的个数； $B_u = [b_{u,1}, b_{u,2}, \dots, b_{u,m}]^T$ ， $b_{u,j} \in \{0,1\}$ 为表达式系数，如果 $b_{u,j} = 1$ ，则表示 T_u 属于函数输出 f_j ，如果有多个 $b_{u,j} = 1$ ，则说明 T_u 被多个函数输出共享。

对于 n 输入、 m 输出的布尔函数 F ，其 DRM 逻辑表达式为：

$$F(x_1, x_2, \dots, x_n) = \bigodot_{u=1}^r (A_u + S_u) \quad (2)$$

式中：“ \bigodot ”表示同或运算； $S_u = \bigvee_{i=1}^n \hat{x}_i$ 为和项； r 为和项的个数； $A_u = [a_{u,1}, a_{u,2}, \dots, a_{u,m}]^T$ ， $a_{u,j} \in \{0,1\}$ 为表达式系数，如果 $a_{u,j} = 0$ ，则表示 S_u 属于函数输出 f_j 。

定义 1 混合 RM-DRM 逻辑是函数的 RM 逻辑与 DRM 逻辑混合表示形式，包括 RM 逻辑部分与 DRM 逻辑部分，其逻辑表达式为：

$$F(x_1, x_2, \dots, x_n) = \left[\bigoplus_{u=1}^t B_u T_u \right] \bigoplus \left[\bigodot_{u=1}^r (A_u + S_u) \right] \quad (3)$$

式(3)中符号的含义与式(1)、式(2)中符号的含义相同，对于混合 RM-DRM 逻辑，其包含的项(乘积项或者和项)数为 $r+t$ 。

1.2 混合 RM-DRM 逻辑的构建

定义 2 给定函数 F ，要构建其混合 RM-DRM 逻辑，就是将函数 F 分解为 2 个不相交的函数 G 和 H ，并且满足 $F = G \oplus H$ ，其中 G 采用 RM 逻辑表示， H 采用 DRM 逻辑表示。

根据定义 2，混合 RM-DRM 逻辑的构建转化为函数的分解问题，并要求分解后的函数 G 适合采用 RM 逻辑来进行表示，而函数 H 则适合采用 DRM 逻辑来进行表示。函数 G 与函数 H 既可以是完全规定函数，也可以是不完全规定函数，本文仅讨论函数 G 与函数 H 都为完全规定函数的情形。

由于函数的立方体表示具有相对较高的效率^[17]，因此本文使用立方体集合表示函数。立方体与乘积项或者和项相对应，采用位置标记法的立方体表示为：

$$c = [i_{c,1}, i_{c,2}, \dots, i_{c,n} | o_{c,1}, o_{c,2}, \dots, o_{c,m}] \quad (4)$$

其中的 $i_{c,l}$ 与 \hat{x}_l 相对应， $o_{c,j}$ 与 f_j 相对应。对于积之和(Sum-Of-Products, SOP)表示与 RM 表示， $i_{c,l} \in \{-, 0, 1\}$ 对

应 $\bar{x}_l \in \{-, \bar{x}_l, x_l\}$, 如果 $o_{c,j}=1$, 则表示 c 对应的乘积项属于 f_j 。对于和之积(Product-Of-Sums, POS)表示与 DRM 表示, $i_{c,l} \in \{-, 1, 0\}$ 对应 $\bar{x}_l \in \{-, \bar{x}_l, x_l\}$, 如果 $o_{c,j}=0$, 则表示 c 对应的和项属于 f_j 。

定义 3 立方体间的距离指的是输入变量在 2 个立方体中以不同形式出现的个数, 使用 $D_{a,b}$ 表示立方体 a 与 b 间的距离, 计算公式为^[17]:

$$D_{a,b} = \sum_{l=1}^n (1 | i_{a,l} \neq i_{b,l}) \quad (5)$$

由于 RM 逻辑常由函数的 SOP 表示获得, 而 DRM 逻辑常由函数的 POS 表示获得^[15], 因此如果给定函数 F 的 SOP 表示, 则先识别出其中适合采用 RM 逻辑表示的部分 G (RM 逻辑部分), 剩余的部分 $H=G \oplus F$ 则视为适合采用 DRM 逻辑表示的部分(DRM 逻辑部分); 如果给定函数的 POS 表示, 则先识别出 DRM 逻辑部分 H , 剩余的部分 $G=H \oplus F$ 则视为 RM 逻辑部分。下面以给定函数的 SOP 表示为例说明混合 RM-DRM 逻辑的构建。

为能较好地识别出给定函数中的 RM 逻辑部分, 本文先由函数的 SOP 表示获得一个初始 RM 覆盖, 然后根据立方体距离对初始 RM 覆盖进行划分。构建混合 RM-DRM 逻辑的步骤如下:

- 1) 采用文献[18]中的方法得到函数 F 的一个初始 ESOP 覆盖, 并将其作为初始 RM 覆盖 C ;
- 2) 将 C 中满足 $D_{a,b}=1$ 或者 $D_{a,b}=2$ 的立方体 a 与 b 划分在立方体集合 C_1 , C_1 为 RM 逻辑部分, 剩余的立方体划分在 $C_2=C \setminus C_1$, C_2 则用来作为 DRM 逻辑部分;
- 3) 对 RM 覆盖 C_2 中的立方体进行不相交运算处理, 得到 SOP 覆盖 C'_2 , 然后再将 C'_2 视为完全规定函数 H 的 ONSET 覆盖, 计算其 OFFSET 覆盖, 并对 OFFSET 覆盖进行不相交运算得到 POS 覆盖 C''_2 ;
- 4) 由于 $C_1 \cup C_2 = C, C_1 \cap C_2 = \emptyset, C_2 \Leftrightarrow C''_2$, 因此覆盖 C_1 是完全规定函数 G 的 RM 逻辑表示, 覆盖 C''_2 则是完全规定函数 H 的 DRM 逻辑表示。

尽管可以将步骤 2) 中的 C_2 作为 DRM 逻辑部分, 但是此时 C_2 实际上仍是 RM 覆盖, 需要将其转换为 DRM 覆盖。由于 DRM 逻辑常由函数的 POS 表示得到, 因此在步骤 3) 中先将 C_2 转换为 SOP 覆盖, 然后再由 SOP 覆盖计算得到 POS 覆盖。由于不相交 SOP 覆盖可以视为一个 RM 覆盖, 不相交 RM 覆盖同样也可以视为一个 SOP 覆盖, 因此对 RM 覆盖 C_2 中的立方体进行不相交运算^[19]处理后, 即可得到 SOP 覆盖 C'_2 。

上述函数分解方法的依据是: C_1 是函数 G 的 RM 覆盖, 其中包含了距离为 1 或 2 的立方体, 可以使用立方体变换进行化简^[17], 因此得到的函数 G 适合采用 RM 逻辑表示。 C_2 是函数 H 的 RM 覆盖, 尽管其中立方体间的距离均大于 2, 但是其 POS 覆盖中应该包含距离为 1 或者 2 的立方体, 也可以使用立方体变换进行化简, 因此得到的函数 H 适合采用 DRM 逻辑表示。故先对覆盖 C_2 中的立方体进行不相交运算得到不相交 SOP 覆盖 C'_2 , 然后再由 C'_2 得到函数 H 的 DRM 覆盖 C''_2 。

1.3 混合 RM-DRM 逻辑的化简与等价性验证

在将函数 F 分解为 2 个不相交的函数 G 和 H , 并分别得到函数 G 的 RM 覆盖 C_1 以及函数 H 的 DRM 覆盖 C''_2 后, 可以使用 RM 逻辑最小化工具分别对其进行化简。

本文使用 EXORCISM-4 工具^[18]对函数 G 进行 RM 逻辑最小化, 利用对偶原理借助 EXORCISM-4 工具对函数 H 进行 DRM 逻辑最小化^[15,20], 从而实现函数 F 的混合 RM-DRM 逻辑化简。

等价性验证是逻辑化简中一个必不可少的阶段, 本文使用基于二元决策图的等价性验证方法^[17]进行混合 RM-DRM 逻辑与原始函数的等价性验证。

2 混合 RM-DRM 逻辑在可逆电路综合中的应用

将 RM 逻辑作为结构表示模型进行可逆电路综合时, 其中的乘积项可以直接映射到 MPMCT 门。而使用 DRM 逻辑作为结构表示模型进行可逆电路综合存在一些缺点: 一是无法将其中文字数大于 2 的和项直接映射为可逆逻辑门, 因为目前暂时没有控制线数大于 2 的或型可逆逻辑门, 二是由于每一个同或运算要转换为异或运算后再进行综合会增加一个 NOT 门, 从而导致量子成本的增加。

为使用混合 RM-DRM 逻辑作为结构表示模型进行可逆电路综合, 在得到函数的混合 RM-DRM 逻辑化简结果后, 先利用对偶原理将其中的 DRM 逻辑表示转换为 RM 逻辑表示, 即, 根据 $x_i + x_j = 1 \oplus \bar{x}_i \bar{x}_j$, 将式(3)中的和项转换为乘积项, 根据 $(x_i + x_j) \odot (x'_k + x'_l) = (1 \oplus \bar{x}_i \bar{x}_j) \oplus x_k x_l$ 将同或运算转换为异或运算, 从而将式(3)所示的混合

RM-DRM 逻辑表示转换为式(1)所示的 RM 逻辑表示, 然后再进行可逆电路综合。这样做的一个好处是可以借助现有的基于 RM 逻辑模型的可逆电路综合中的方法将乘积项映射为 MPMCT 门。

基于混合 RM-DRM 逻辑模型的可逆电路综合方法的步骤如下:

- 1) 构建函数的混合 RM-DRM 逻辑;
- 2) 使用 EXORCISM-4 工具对混合 RM-DRM 逻辑进行最小化;
- 3) 将混合 RM-DRM 逻辑表示转换为 RM 逻辑表示, 并进行等价性验证;
- 4) 使用基于 RM 逻辑模型的可逆电路综合方法进行可逆电路综合。

关于步骤 4)中的可逆电路综合方法可以使用当前文献中将 RM 逻辑作为结构表示模型的可逆电路综合方法, 本文采用文献[21]中的方法对基于混合 RM-DRM 逻辑模型的可逆电路综合方法进行验证。

尽管文献[21]采用的是 ESOP 表示模型, 但由于 ESOP 是 RM 逻辑最一般化的表示形式, 同时为了描述方便, 也将 ESOP 表示模型称为 RM 逻辑模型。

3 实验结果及分析

基于混合 RM-DRM 逻辑模型的可逆电路综合算法采用 C 语言实现, 在 Linux 下使用 gcc 编译器进行编译。根据文献[21]中 MPMCT 门的量子成本计算模型, 使用基于混合 RM-DRM 逻辑模型的可逆电路综合算法对 RevLib 库中的 134 个函数^[16]进行了可逆电路综合。下面给出主要结果, 并对结果进行分析, 从而给出一些重要结论。

与文献[21]中直接使用 RM 逻辑作为结构表示模型进行可逆电路综合相比, 采用混合 RM-DRM 逻辑作为结构表示模型综合所得可逆电路:

- 1) 对于一个 n 输入 m 输出的函数, 其量子位数同样为 $n+m$ 。
- 2) 在 134 个函数中, 有 60 个函数其可逆电路的量子成本得以降低, 62 个函数其可逆电路的量子成本有所提高, 12 个函数其可逆电路的量子成本相同。
- 3) 有 25 个函数量子成本降低的比例超过了 10%, 如图 1 所示, 其中有 9 个函数量子成本降低的比例超过了 20%, 其中函数 urf4 量子成本降低的比例为 33.36%, 函数 parity 量子成本降低的比例则高达 43.75%。

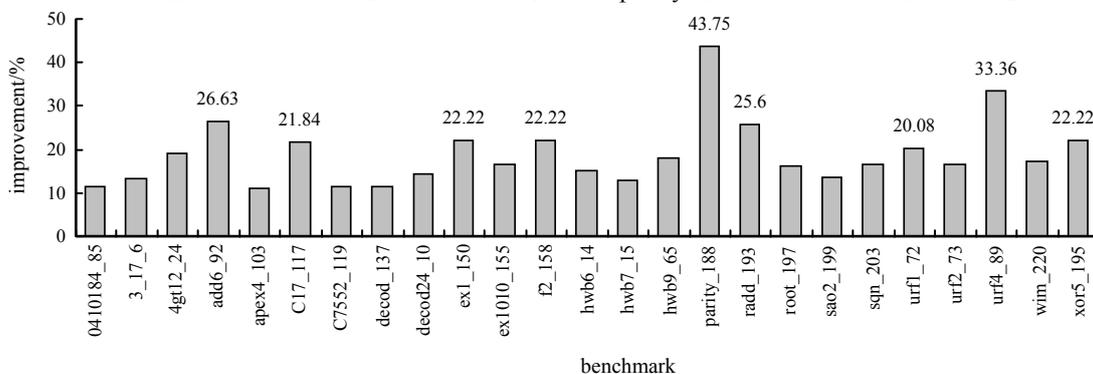


Fig.1 Improvement for the quantum cost of reversible circuits
图 1 可逆电路量子成本改进结果

对于函数 parity, 采用 RM 逻辑模型进行逻辑最小化得到的结果包含 16 个单文字乘积项, 这 16 个乘积项中变量的出现形式均为负极性(\bar{x}_i), 综合所得可逆电路的量子成本为 32; 采用混合 RM-DRM 逻辑模型进行逻辑最小化, 并利用对偶原理转换为 RM 逻辑表示所得到的结果包含 1 个常量乘积项和 16 个单文字乘积项, 其中仅有 1 个乘积项包含负极性的变量, 综合所得可逆电路的量子成本为 18。这是因为对于一个 MPMCT 门, 当其所有控制线均为负控制线时, 其 NCV 实现的量子成本要有所增加^[6]。

4) 尽管并不能使所有函数综合所得可逆电路都能够获得量子成本的降低, 但从 134 个 RevLib 函数的平均结果来看, 混合 RM-DRM 逻辑模型的采用使得综合所得可逆电路的量子成本降低了 4.93%。

与采用 RM 逻辑模型相比, 采用混合 RM-DRM 逻辑模型能够降低综合所得可逆电路的量子成本的原因有以下几个方面:

- 1) 输出等价类中的立方体数量有所增加, 当乘积项在多个函数输出之间的共享比较突出时, 此因素有助于降低量子成本。

2) 乘积项在多个函数输出之间的共享有所减弱, 当乘积项在多个函数输出之间的共享不明显时, 此因素有助于降低量子成本。

3) 乘积项间的结构相似性有所提高, 这有助于通过立方体聚类提取多个乘积项间的公因子^[21], 从而降低量子成本。

4) 乘积项中负极性变量的数量减少, 这使得所有变量均为负极性的乘积项的数量减少, 也减少了所有控制线均为负控制线的 MPMCT 门数量, 从而有助于降低量子成本。

另外, 在将多输出函数作为一个整体进行可逆电路综合时, 由于可逆电路中不允许直接使用扇出, 再加上量子位硬件资源的限制, 除现有的 $n+m$ 条线外, 不再增加辅助线, 而是使用电路中已有的线作为临时辅助线来映射乘积项, 并借助复制门(CNOT 门)使乘积项映射所得 MPMCT 门或可逆子电路在尽可能多的输出变量线(保存函数输出变量状态的线)之间共享^[21]。尽管一个乘积项被多个函数输出共享, 但如果电路中没有临时辅助线可用, 则无法借助复制门实现乘积项映射所得 MPMCT 门或可逆子电路的共享, 因此乘积项在多个函数输出间的共享度的增加并不一定意味着量子成本的降低。这也是为何当一个函数的最小混合 RM-DRM 逻辑表示中的乘积项数比该函数的最小 RM 逻辑表示中的乘积项数多时, 采用混合 RM-DRM 逻辑模型进行可逆电路综合却能够降低该函数综合所得可逆电路的量子成本的一个原因。

4 结论

RM 逻辑与 DRM 逻辑互为对偶表示, 将一个函数同时采用 RM 逻辑与 DRM 逻辑进行表示, 有可能获得成本较低的电路。本文提出了混合 RM-DRM 逻辑模型, 介绍了混合 RM-DRM 逻辑的一种构建方法以及一种化简方法。将混合 RM-DRM 逻辑作为结构表示模型应用于可逆电路综合, 给出了基于混合 RM-DRM 逻辑模型的可逆电路综合方法, 并使用 RevLib 库中的函数对综合方法进行了验证。可逆电路综合的结果表明, 与采用 RM 逻辑作为表示模型相比, 在不增加量子位数的前提下, 采用混合 RM-DRM 逻辑模型能够降低某些函数综合所得可逆电路的量子成本, 并且将 134 个 RevLib 函数综合所得可逆电路的平均量子成本降低了 4.93%。降低可逆电路的量子成本, 有助于降低可逆电路的量子电路实现的计算复杂度。

本文只是介绍了混合 RM-DRM 逻辑的一种构建方法以及一种化简方法, 如何更好地识别函数中的 RM 逻辑部分以及 DRM 逻辑部分, 从而更好地构建混合 RM-DRM 逻辑, 以及如何将可逆电路的量子成本作为标准来指导混合 RM-DRM 逻辑的化简则是下一步的研究工作。

参考文献:

- [1] RAHAMAN H,DAS D K,BHATTACHARYA B B. Testable design of AND-EXOR logic networks with universal test sets[J]. Computers and Electrical Engineering, 2009,35(5):644-658.
- [2] MONTEIRO C,TAKAHASHI Y,SEKINE T. Low-power secure S-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design[J]. IET Circuits, Devices & Systems, 2015,9(5):362-369.
- [3] KUMAR S D,THAPLIYAL H,MOHAMMAD A. FinSAL: FinFET based secure adiabatic logic for energy-efficient and DPA resistant IoT devices[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018,37(1): 110-122.
- [4] DRECHSLER R,WILLE R. Synthesis of reversible circuits using decision diagrams[C]// Proceedings of the International Symposium on Electronic System Design. Kolkata,India:IEEE, 2012:1-5.
- [5] NIELSEN M A,CHUANG I L. Quantum computation and quantum information[M]. 10th anniversary ed. New York: Cambridge University Press, 2010.
- [6] ABDESSAIED N,DRECHSLER R. Reversible and quantum circuits: optimization and complexity analysis[M]. Bremen, Germany:Springer Press, 2016.
- [7] ZULEHNER A,WILLE R. Skipping embedding in the design of reversible circuits[C]// Proceedings of the IEEE 47th International Symposium on Multiple-Valued Logic. Novi Sad,Serbia:IEEE, 2017:173-178.
- [8] YOUNES A,MILLER J F. Representation of Boolean quantum circuits as Reed-Muller expansions[J]. International Journal of Electronics, 2004,91(7):431-444.
- [9] FAZEL K,THORNTON M A,RICE J E. ESOP-based Toffoli gate cascade generation[C]// Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. Victoria,BC,Canada:IEEE, 2007:206-209.

- [10] BARENCO A,BENNETT C H,CLEVE R,et al. Elementary gates for quantum computation[J]. *Physical Review A*, 1995, 52(5):3457–3467.
- [11] YANG G,XIE F,HUNG W N N,et al. Realization and synthesis of reversible functions[J]. *Theoretical Computer Science*, 2011,412(17):1606–1613.
- [12] 陈汉武,李文骞,阮越,等. 基于汉明距离递减变换的可逆逻辑综合算法[J]. *计算机学报*, 2014,37(8):1839–1845. (CHEN Hanwu,LI Wenqian,RUAN Yue,et al. A synthesis algorithm of reversible logic circuit based on the decreasing transform of Hamming distance[J]. *Chinese Journal of Computers*, 2014,37(8):1839–1845.)
- [13] SOEKEN M,WILLE R,KESZOCZE O,et al. Embedding of large Boolean functions for reversible logic[J]. *ACM Journal on Emerging Technologies in Computing Systems*, 2016,12(4):41:1–41:26.
- [14] 王友仁,沈先坤,周影辉. 基于 KFDD 的可逆逻辑电路综合设计方法[J]. *电子学报*, 2014,42(5):1025–1029. (WANG Youren,SHEN Xiankun,ZHOU Yinghui. Synthesis design method of reversible logic circuit based on Kronecker functional decision diagram[J]. *Acta Electronica Sinica*, 2014,42(5):1025–1029.)
- [15] 卜登立,江建慧. 基于对偶逻辑的混合极性 RM 电路极性转换和优化方法[J]. *电子学报*, 2015,43(1):79–85. (BU Dengli,JIANG Jianhui. Dual logic based polarity conversion and optimization of mixed polarity RM circuits[J]. *Acta Electronica Sinica*, 2015,43(1):79–85.)
- [16] WILLE R,GROBE D,TEUBER L,et al. RevLib: an online resource for reversible functions and reversible circuits[C]// *Proceedings of the 38th International Symposium on Multiple-Valued Logic*. Dallas,TX:IEEE, 2008:220–225.
- [17] 卜登立. 快速启发式 ESOP 电路面积优化算法[J]. *计算机辅助设计与图形学学报*, 2015,27(11):2161–2168. (BU Dengli. Fast heuristic area optimization algorithm for ESOP circuits[J]. *Journal of Computer-Aided Design & Computer Graphics*, 2015,27(11):2161–2168.)
- [18] MISHCHENKO A,PERKOWSKI M. Fast heuristic minimization of exclusive-sums-of-products[C]// *Proceedings of Reed–Muller Workshop*. Mississippi,USA:IEEE, 2001:242–250.
- [19] BU Dengli,JIANG Jianhui. An efficient optimization algorithm for multi-output MPRM circuits with very large number of input variables[C]// *Proceedings of the IEEE 7th Joint International Information Technology and Artificial Intelligence Conference*. Chongqing,China:IEEE, 2014:228–232.
- [20] 卜登立,胡运全,廖萍. Exclusive-nor sum-of-sum 逻辑及其最小化研究[J]. *井冈山大学学报(自然科学版)*, 2017, 38(5):39–45. (BU Dengli,HU Yunquan,LIAO Ping. Research on exclusive-nor sum-of-sum logic and its minimization[J]. *Journal of Jinggangshan University(Natural Science)*, 2017,38(5):39–45.)
- [21] 卜登立. 基于 ESOP 最大加权输出相容类的可逆电路综合方法[J]. *电子学报*, 2018,46(8):1866–1875. (BU Dengli. Reversible circuit synthesis method based on maximum weighted output-compatibility class of ESOP[J]. *Acta Electronica Sinica*, 2018,46(8):1866–1875.)

作者简介:



卜登立(1975–), 男, 河北省定州市人, 博士, 副教授, 主要研究方向为可逆逻辑综合、量子电路综合、启发式优化算法.email:bodengli@163.com.