# 基于概率表达式的 MPRM 电路功耗计算方法

卜登立[1,2]

(1. 井冈山大学电子与信息工程学院,江西吉安 343009;
2. 流域生态与地理环境监测国家测绘地理信息局重点实验室,江西吉安 343009)

**摘 要:** 采用基于信号概率的功耗计算模型进行 MPRM(Mixed Polarity Reed-Muller)电路功耗优化,信号概率计算是功耗计算的关键.提出一种基于概率表达式的 MPRM 电路功耗计算方法.该方法兼顾信号概率计算的时间效率和准确性,对 MPRM 电路中不存在空间相关性的信号通过在电路中传播信号概率的方式计算其信号概率,存在空间相关性的信号则利用概率表达式计算其信号概率,并在电路中传播概率表达式以解决空间相关性问题,在此基础之上根据基于信号概率建立的解析动态功耗和静态功耗计算模型计算电路功耗.为进一步提高时间效率,该方法采用二元矩图表示概率表达式.使用基准电路对所提出方法进行了验证,并与其他采用不同信号概率计算方法的 MPRM 电路功耗计算方法进行了比较.结果表明所提出方法准确有效.

**关键词:** MPRM 电路;功耗计算;信号概率;空间相关;概率表达式;二元矩图

**中图分类号:** TP391.72 **文献标识码:** A **文章编号:** 0372-2112 (2018)12-3060-08

**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.12.033

# Probability Expression Based Power Estimation Method for MPRM Circuits

BU Deng-li[1,2]

(1. *School of Electronics and Information Engineering, Jinggangshan University, Ji'an, Jiangxi* 343009, *China*;
2. *Key Laboratory of Watershed Ecology and Geographical Environment Monitoring, NASG, Ji'an, Jiangxi* 343009, *China*)

**Abstract:** Signal probability calculation is the key to power estimation when optimizing power of MPRM (Mixed Polarity Reed-Muller) circuits by using signal probability based power estimation models. A probability expression based power estimation method is proposed for MPRM circuits. The proposed method takes into account both efficiency and accuracy of signal probability calculation, for signals having not spatial correlation in MPRM circuit, their signal probabilities are computed by means of signal probability propagation in circuit, whereas for signals having spatial correlation, probability expressions are utilized to calculate their signal probabilities and are propagated in circuit to resolve spatial correlation problem, then the dynamic and static power of the circuit are computed respectively by using the established analytical power estimation models based on signal probability. In order to further improve time efficiency, the proposed method utilizes binary moment diagram to represent probability expression. The proposed method is validated by using several benchmark circuits, and compared to other power estimation methods using different signal probability calculation methods for MPRM circuits. Results show that the proposed method is accurate and effective.

**Key words:** MPRM circuits; power estimation; signal probability; spatial correlation; probability expression; binary moment diagram

## 1 引言

Reed-Muller(RM)逻辑是函数基于 AND/XOR 的逻辑表示,与基于 AND/OR 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,并且能够实现具有通用测试集的可测试性电路设计[1].近几年来 RM 逻辑在信息安全领域的电路设计中的实际应用,如 AES 加密电路中的 S 盒电路[2]、基于 FinFET 的安全绝

收稿日期:2017-05-26;修回日期:2018-06-24;责任编辑:梅志强
基金项目:国家自然科学基金(No. 61640412, No. 61762052);江西省教育厅科技计划项目(No. GJJ160746);流域生态与地理环境监测国家测绘地理信息局重点实验室资助课题(No. WE2016012);井冈山大学博士科研启动项目(No. JZB1803);江西省自然科学基金项目(No. 20171BAB202010)

热电路[3]等,验证了对 RM 电路进行功耗、可靠性等优化的必要性.

近年来,RM 电路的功耗优化问题得到了较多关注,如文献[4]进行混合极性 RM(Mixed Polarity RM, MPRM)电路的动态功耗优化,文献[5]进行三进制固定极性 RM 电路的面积与动态功耗优化,文献[6]借助 RM 决策图对 RM 电路进行面积与动态功耗优化,文献[7]进行 MPRM 电路的面积与动态功耗优化,文献[8]则针对不完全规定函数进行 MPRM 电路的面积、动态功耗与静态功耗多目标优化. 这些文献都采用基于信号概率的解析功耗计算模型计算电路的功耗,由于功耗与电路中节点的信号概率有关,因此信号概率的计算成为功耗计算的关键. 但除文献[4,8]外的其他文献都忽略信号间的相关性,采用直接在电路中传播信号概率的方法计算信号概率. 文献[4]考虑信号的时间相关性,并采用二元决策图(Binary Decision Diagram, BDD)法[9]计算信号概率. 电路中扇出以及重汇聚的存在,导致了电路中信号间的空间相关,忽略空间相关性将导致信号概率计算和电路功耗计算的误差.

本文针对电路中信号间的空间相关性问题,提出一种基于概率表达式的 MPRM 电路功耗计算方法. 该方法对电路中不存在空间相关性的信号通过在电路中传播信号概率的方式计算其信号概率,对存在空间相关性的信号则利用概率表达式法计算其信号概率,且在底层使用二元矩图表示概率表达式,目的是兼顾信号概率计算的时间效率以及准确性. 给出了 MPRM 电路的基于信号概率的解析功耗计算模型以及基于概率表达式的 MPRM 电路功耗计算算法,使用基准电路对算法进行了验证,并与其他采用不同信号概率计算方法的 MPRM 电路功耗计算方法进行了比较.

## 2　信号概率计算

下面先简要介绍 MPRM 逻辑,然后介绍信号概率计算方法. 本文信号概率的计算基于零延迟模型以及信号时间不相关假设.

### 2.1　MPRM 逻辑

假设布尔函数具有 $n$ 个输入变量 $\{x_i|1\le i\le n\}$、$m$ 个输出变量 $\{f_o|1\le o\le m\}$,输入变量 $x_i$ 也被称为原始输入(Primary Input, PI)和 PI 信号,输出变量 $f_o$ 也被称为原始输出(Primary Output, PO)和 PO 信号. 其关于 PI 的 MPRM 逻辑表达式如式(1)所示.

$$\boldsymbol{F}(x_1,x_2,\cdots,x_n)=\bigoplus_{u=1}^{t}\boldsymbol{B}_u T_u \tag{1}$$

其中 $\boldsymbol{F}=[f_1,f_2,\cdots,f_m]^{\mathrm{T}}$,"$\oplus$"表示异或运算;$T_u=\bigwedge_{i=1}^{n}\hat{x}_i$ 为乘积项,$\hat{x}_i\in\{-,x_i,\bar{x}_i\}$,如果 $\hat{x}_i\neq -$,则称其为 $T_u$ 中的一个文字,$\hat{x}_i=x_i$ 时记作 $x_i\in T_u$,$\hat{x}_i=\bar{x}_i$ 时记作 $\bar{x}_i\in T_u$,$t$ 则为乘积项的个数. $\boldsymbol{B}_u=[b_{u,1},b_{u,2},\cdots,b_{u,m}]^{\mathrm{T}}$,$b_{u,o}\in\{0,1\}$为表达式系数,如果 $b_{u,o}=1$,则表示 $T_u$ 存在于 $f_o$ 的逻辑表达式中,记作 $T_u\in f_o$.

**定义 1**　对于 $T_u$ 和 $T_w$($1\le u,w\le t,u\neq w,T_u\in f_o\wedge T_w\in f_o$),如果 $x_i\in T_u\wedge x_i\in T_w$ 或者 $\bar{x}_i\in T_u\wedge\bar{x}_i\in T_w$,则称 $T_u$ 和 $T_w$ 存在着关于 PI 信号 $x_i$ 的空间相关性. 满足此条件的 $x_i$ 越多,则 $T_u$ 和 $T_w$ 关于 PI 信号的空间相关性越强.

但如果 $x_i\in T_u\wedge\bar{x}_i\in T_w$,由于信号 $x_i$ 与 $\bar{x}_i$ 互斥,则此时可以认为 $T_u$ 和 $T_w$ 不存在关于 PI 信号 $x_i$ 的空间相关性.

本文假设所有 PI 信号是空间相互独立的,即不存在空间相关性. 为描述方便,以下本文中的"信号相互独立"指的是"信号空间相互独立","信号相关"指的是"信号空间相关".

### 2.2　基于概率表达式的信号概率计算

**定义 2**　逻辑信号 $x_i$ 的信号概率 $X_i=\Pr(x_i=1)$是 $x_i$ 取值为 1 的概率,$X_i\in[0,1]$为实值随机变量.

为简化描述,以下使用 $\Pr(x_i)$表示 $\Pr(x_i=1)$.

**定义 3**　A 变换将逻辑信号 $x_i$ 从布尔域变换到实数域,即 $\mathrm{A}(x_i)=X_i$.

**定理 1**　对于信号 $x_i$ 和 $x_j$,假设他们相互独立,则以下 A 变换成立[10,11]:

$$\begin{cases}\mathrm{A}(\bar{x}_i)=1-\mathrm{A}(x_i)=1-X_i\\ \mathrm{A}(x_i\wedge x_j)=X_iX_j\\ \mathrm{A}(x_i\oplus x_j)=X_i+X_j-2X_iX_j\end{cases}\tag{2}$$

**定义 4**　关于定义 2 中随机变量的多项式表示称之为概率表达式.

如式(2)中的 $X_i+X_j-2X_iX_j$ 则是关于 $X_i$ 和 $X_j$ 的概率表达式. 将 $X_i$ 和 $X_j$ 的值 $\Pr(x_i)$和 $\Pr(x_j)$代入式(2)即可得到如式(3)所示的信号概率求值公式.

$$\begin{cases}\Pr(\bar{x}_i)=1-\Pr(x_i)\\ \Pr(x_i\wedge x_j)=\Pr(x_i)\Pr(x_j)\\ \Pr(x_i\oplus x_j)=\Pr(x_i)+\Pr(x_j)-2\Pr(x_i)\Pr(x_j)\end{cases}\tag{3}$$

现假设电路的逻辑函数及其 PO 均使用 $f$ 表示,电路包含 $g$ 个逻辑门$\{g_k|1\le k\le g\}$,逻辑门 $g_k$ 的输出信号也使用 $g_k$ 表示. 在计算信号概率之前,需从 PI 至 PO 方向对电路 $f$ 进行拓扑排序.

**定义 5**　简单信号概率计算法. 假设电路 $f$ 中的信号间不存在相关性,按拓扑排序根据逻辑门 $g_k$ 关于其输入信号的逻辑函数由式(3)计算信号 $g_k$ 的信号概率 $\Pr(g_k)$,并向将信号 $g_k$ 作为输入的逻辑门传播 $\Pr(g_k)$,最终计算出 $f$ 的信号概率 $\Pr(f)$.

定义 5 的简单信号概率计算法是当前 RM 电路功

耗优化研究工作中普遍采用的信号概率计算方法，如文献[6,7]. 当电路中的信号间存在相关性时，简单信号概率计算法将会导致信号概率计算结果的误差.

**定义 6** 信号概率计算的概率表达式法. 按拓扑排序根据定理 1 对逻辑门 $g_k$ 的逻辑函数进行 A 变换，并在该过程中利用幂等律拟制 PI 信号随机变量的指数成分得到信号 $g_k$ 的概率表达式 $\mathrm{A}(g_k)$，同时向将信号 $g_k$ 作为输入的逻辑门传播 $\mathrm{A}(g_k)$，最终得到函数 $f$ 的概率表达式 $\mathrm{A}(f)$，将 PI 信号随机变量的值代入 $\mathrm{A}(g_k)$ 和 $\mathrm{A}(f)$ 即可计算得到 $\Pr(g_k)$ 和 $\Pr(f)$.

定义 6 中的 $\mathrm{A}(g_k)$ 和 $\mathrm{A}(f)$ 是关于 PI 信号随机变量的多项式表示，概率表达式的传播，以及在 A 变换过程中对 PI 信号随机变量指数成分的抑制很好地处理了信号间的相关性[10]，因此概率表达式法可以得到准确的信号概率结果.

### 2.3 二元矩图

二元矩图（Binary Moment Diagram，BMD）[12]是具有实数、有理数或者整数值函数的图形表示，常被用来进行算术电路的验证. 在使用 BMD 表示概率表达式时，使用终端结点表示表达式系数，非终端结点表示变量.

对于逻辑函数 $f = x_1x_2 \oplus x_2x_3$，根据式（2）对其进行 A 变换并抑制随机变量的指数成分可以得到 $\mathrm{A}(f) = X_1X_2 + X_2X_3 - 2X_1X_2X_3$，图 1 给出了 $\mathrm{A}(f)$ 的 BMD 表示.

图 1 所示的 BMD 也可以看作是依据矩对函数 $f = x_1x_2 \oplus x_2x_3$ 进行的线性分解[12]，结点的实线边表示函数 $f$ 随该变量线性变化的部分，而虚线边则表示函数 $f$ 不依赖于该变量的部分.

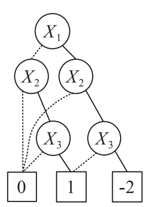

图1 BMD示例

BMD 提供了支持定理 1 中对函数进行 A 变换的算术运算[12]，如 $\mathrm{A}(x_i \wedge x_j)$ 通过算术与实现，$\mathrm{A}(x_i \oplus x_j)$ 通过算术异或实现，并且可以实现定义 6 中的“在 A 变换过程中利用幂等律抑制随机变量的指数成分”. 对函数 $f$ 的逻辑表达式实施相应的算术运算即可得到 $\mathrm{A}(f)$ 对应的 BMD，将随机变量 $X_i$ 的值代入，进行 BMD 求值[12]即可得到 $f$ 的信号概率. BMD 可以较高效率地表示和操纵类似于概率表达式的代数表达式，并且 BMD 求值的复杂度为线性复杂度[12]，因此本文在底层使用 BMD 表示概率表达式.

## 3 MPRM 电路功耗计算

电路功耗包括动态功耗和静态功耗[13]，基于零延迟假设，动态功耗常使用电路开关活动进行评价[4~7]，而静态功耗常采用电路泄漏电流进行评价[8,13,14]. 假设电路包括 $g$ 个逻辑门，第 $k$ 个逻辑门及其输出信号使用 $g_k$ 表示，由文献[6]可以得到如式（4）所示的电路开关活动计算公式，也称其为动态功耗计算公式. 假设逻辑门 $g_k$ 的输入数为 $I_k$，其第 $l$ 个输入信号使用 $s_{k,l}$ 表示，由文献[14]可以得到如式（5）所示的电路泄漏电流计算公式，也称其为静态功耗计算公式.

$$E_{\mathrm{d}} = \sum_{k=1}^{g} 2\Pr(g_k)(1 - \Pr(g_k)) \tag{4}$$

$$E_{\mathrm{s}} = \sum_{k=1}^{g} \left( \sum_{v=0}^{2^{I_k-1}} P_{k,v} L_{k,v} \right) \tag{5}$$

式（5）中的 $P_{k,v}$ 表示逻辑门 $g_k$ 的输入信号在组合值为 $v$ 时的联合信号概率，即 $P_{k,v} = \Pr(\bigwedge_{l=1}^{I_k} \tilde{s}_{k,l})$，其中 $\tilde{s}_{k,l} \in \{s_{k,l}, \bar{s}_{k,l}\}$，$v = \sum_{l=1}^{I_k} (2^{l-1} c_l) \left| c_l = \begin{cases} 1, \tilde{s}_{k,l} = s_{k,l} \\ 0, \tilde{s}_{k,l} = \bar{s}_{k,l} \end{cases} \right.$；$L_{k,v}$ 则表示逻辑门 $g_k$ 在输入信号的组合值为 $v$ 时的泄漏电流. 式（5）所示的静态功耗计算公式考虑了输入向量对电路静态功耗的影响.

本文采用与文献[15]类似的 MPRM 电路模型，将 MPRM 电路分为输入部分、AND 部分和 XOR 部分，如图 2（$a$）所示，其中的“$\oplus$”表示异或门. AND 部分中的 $T_u$ 对应如式（1）所示 MPRM 逻辑表达式中的乘积项，XOR 部分则完成乘积项间的异或运算，输入部分的非门仅在 $T_u$ 中包含 $\bar{x}_i$ 时才存在. 对于 XOR 部分，使用文献[15]中的异或门分解算法将其分解为树形 2 输入异或门网络；对于 AND 部分的处理则与文献[15]有所不同，为降低电路的延时，本文将 $T_u$ 分解为平衡树形结构的 2 输入与门网络，假设图 2（$a$）中的 $T_t$ 包含 5 个文字，则可将其分解为如图 2（$b$）所示的 4 个 2 输入与门. 另外，为降低电路的面积，本文采用类似于文献[15]中的异或门分解方法对宏门 $T_u$ 进行平衡树分解来实现 2 输入与门的共享.

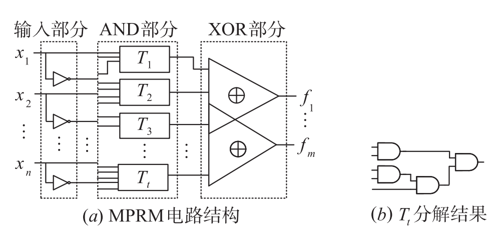

图2 MPRM电路模型

由式（4）和（5）计算 MPRM 电路的动态功耗和静态功耗，需计算逻辑门 $g_k$ 的信号概率 $\Pr(g_k)$ 和 $P_{k,v}$. 为兼顾信号概率计算的时间效率以及准确性，在计算信号概率时，对 MPRM 电路中不存在相关性的信号采用简单信号概率计算法，对存在相关性的信号则采用概率

表达式法.

MPRM 电路输入部分中非门信号概率的计算采用简单信号概率计算法. AND 部分中 $T_u$ 的输入信号间不存在相关性，因此树形分解后的与门的输入信号间也不存在相关性，故与门信号概率的计算也采用简单信号概率计算法. 由于 MPRM 逻辑的乘积项间可能存在着定义 1 所述的关于 PI 信号的相关性，导致分解后的异或门的输入信号之间存在着关于 PI 信号的相关性，因此 XOR 部分中异或门信号概率的计算采用概率表达式法. 如果异或门的输入信号是图 2($a$)中 $T_u$ 的输出信号，则在构建该异或门的概率表达式计算信号概率前，还需构建并传播 $T_u$ 的概率表达式. 下面给出基于概率表达式的 MPRM 电路功耗计算算法.

**算法 1　基于概率表达式的 MPRM 电路功耗计算算法**

Step1：建立逻辑门泄漏电流 $L_{k,v}$ 的表格；
Step2：读取 MPRM 逻辑的 PLA 格式文件；
Step3：如果有一个 $T_u$ 包含 $\bar{x}_i$，则在输入部分增加一个非门；
Step4：将 AND 部分的 $T_u$ 分解为 2 输入与门网络，将 XOR 部分分解为 2 输入异或门网络；
Step5：从 PI 至 PO 方向对电路进行拓扑排序；
Step6：使用简单信号概率计算法计算非门和与门的信号概率 $P_{k,v}$ 和 $\Pr(g_k)$；
Step7：采用概率表达式法计算异或门的信号概率 $P_{k,v}$ 和 $\Pr(g_k)$；
Step8：根据 $\Pr(g_k)$ 由式(4)计算 $E_d$，根据 $P_{k,v}$ 并查询 $L_{k,v}$ 表格由式(5)计算 $E_s$.

算法 1 的 Step2 所需的 MPRM 逻辑的 PLA 格式文件由基于有向 Kronecker 功能决策图的 MPRM 极性转换方法[15]得到. Step7 中的概率表达式采用 BMD 表示.

基于信号概率计算电路的功耗，其准确性依赖于信号概率计算的准确性. 为验证算法 1 功耗计算的准确性，采用电路逻辑模拟的方法得到 MPRM 电路中 $P_{k,v}$ 和 $\Pr(g_k)$ 的准确计算结果，以得到电路功耗的准确计算结果，如算法 2 所示.

**算法 2　基于逻辑模拟法的 MPRM 电路功耗计算算法**

Step1 ~ Step5：与算法 1 的 Step1 ~ Step5 相同；
Step6：在电路的原始输入穷举应用所有输入向量，通过对电路进行逻辑模拟得到电路中所有节点的逻辑信号值；
Step7：根据各个电路节点的逻辑信号值计算出逻辑门 $g_k$ 的信号概率 $P_{k,v}$ 和 $\Pr(g_k)$；
Step8：根据 $\Pr(g_k)$ 由式(4)计算 $E_d$，根据 $P_{k,v}$ 并查询 $L_{k,v}$ 表格由式(5)计算 $E_s$.

按信号概率计算方法的不同，当前基于信号概率的 RM 电路功耗计算方法主要有 2 类：第一类方法使用简单信号概率计算法计算所有的信号概率，如文献[6，7]；第二类方法采用在 BDD 中传播信号概率的 BDD 法计算信号概率，如文献[4]在解决信号的时间相关性问题时就采用了类似方法. 为与这 2 类方法进行比较，分别设计如算法 3 所示以及如算法 4 所示的 MPRM 电路功耗计算算法.

**算法 3　基于简单信号概率计算的 MPRM 电路功耗计算算法**

Step1 ~ Step6：与算法 1 的 Step1 ~ Step6 相同；
Step7：使用简单信号概率计算法计算异或门的信号概率 $P_{k,v}$ 和 $\Pr(g_k)$；
Step8：根据 $\Pr(g_k)$ 由式(4)计算 $E_d$，根据 $P_{k,v}$ 并查询 $L_{k,v}$ 表格由式(5)计算 $E_s$.

算法 4 的 Step4 在计算逻辑门 $g_k$ 的信号概率时，根据其输入组合信号 $\bigwedge_{l=1}^{l_k} \tilde{s}_{k,l}$ 关于 PI 的 BDD 计算 $P_{k,v}$，根据其输出信号 $g_k$ 关于 PI 的 BDD 计算 $\Pr(g_k)$. 由 BDD 计算信号概率的理论依据是由香农分解原理得出的 $\Pr(f) = \Pr(x_i)\Pr(f_{x_i}) + \Pr(\bar{x}_i)\Pr(f_{\bar{x}_i})$ [9,16]，其中 $f_{x_i}$ 和 $f_{\bar{x}_i}$ 分别为对 $x_i$ 实施香农分解后的正、负余子式.

**算法 4　基于 BDD 法的 MPRM 电路功耗计算算法**

Step1：建立逻辑门泄漏电流 $L_{k,v}$ 的表格；
Step2：读取分解后的 MPRM 电路网表；
Step3：从 PI 至 PO 方向对电路进行拓扑排序；
Step4：对电路中的每一个逻辑门 $g_k$，采用 BDD 法计算 $\Pr(g_k)$ 和 $P_{k,v}$；
Step5：根据 $\Pr(g_k)$ 由式(4)计算 $E_d$，根据 $P_{k,v}$ 并查询 $L_{k,v}$ 表格由式(5)计算 $E_s$.

## 4　实验及结果分析

算法 1、算法 2 和算法 3 采用 C + + 语言实现，在 Linux 下使用 g + + 编译器编译；算法 4 则采用 C 语言实现，在 Linux 下使用 gcc 编译器编译. 使用 MCNC 和 ITC99 基准电路在配置为 Intel Core i7-6500U CPU 8GB RAM 的个人计算机上对算法 1 进行验证，并与其他采用不同信号概率计算方法的 MPRM 电路功耗计算方法进行比较.

### 4.1　实验设置

为评价基于概率表达式的 MPRM 电路功耗计算方法，实施了 2 组实验. 第一组实验使用一组输入数较少的 MCNC 基准电路来比较算法 1 和算法 2 的结果，用于验证算法 1 功耗计算的准确性. 第二组实验则使用一组输入数大于 14 的 ITC99 和 MCNC 基准电路来比较算法 1、算法 3、算法 4 以及功耗计算工具 ACE2. 0[16]. 本文中 ACE2. 0 采用 BDD 符号模拟法计算 MPRM 电路中逻辑门的信号概率，并根据式(4)和(5)计算电路的动态功耗和静态功耗. 算法 4 和 ACE2. 0 所读取的 MPRM 电路

网表为对 MPRM 逻辑进行分解后的 BLIF[17] 格式的电路网表,该网表事先由算法 1 的 Step2 ~ Step4 生成.

为使实验结果更具有说服力,对于每一个基准电路,先随机生成 100 个不同的极性值,然后分别计算这 100 个极性值的 MPRM 电路的动态功耗和静态功耗,并分别统计动态功耗和静态功耗的平均值,以及功耗计算所需时间的平均值. 关于功耗计算时间,算法 1、算法 2 和算法 3 为 Step5 ~ Step8 的执行时间,算法 4 为 Step3 ~ Step5 的执行时间,ACE2.0 则为构建 BDD 并通过符号模拟计算信号概率以及根据式(4)和(5)计算功耗所需的时间. 算法 1、算法 3、算法 4 和 ACE2.0 中电路 PI 的信号概率均为 0.5,关于计算静态功耗所需的逻辑门泄漏电流,本文使用文献[13]中 22nm 工艺下的逻辑门由 SPICE 模拟得出的泄漏电流结果,该结果考虑了晶体管的堆叠效应和负载效应.

### 4.2 算法 1 功耗计算的准确性验证

对一组 MCNC 基准电路,分别使用算法 1 和算法 2 计算其 MPRM 电路的功耗,表 1 给出了结果,其中“I/O”表示电路的 PI 数和 PO 数;$E_d$ 和 $E_s$ 则是对每一个基准电路,其 100 个 MPRM 电路的动态功耗以及静态功耗计算结果的平均值,$E_s$ 的单位是 μA;时间为 100 个 MPRM 电路功耗计算时间的平均值,单位为秒.

对于表 1 中的这些电路,无论是动态功耗还是静态功耗,算法 1 的结果均与算法 2 相同. 针对每一个基准电路做进一步分析,对于每一个极性值相同的 MPRM 电路,算法 1 均能得到与算法 2 相同的动态功耗和静态功耗计算结果(因空间关系,这里不再给出每一个 MPRM 电路的功耗计算结果),这验证了算法 1 功耗计算结果的准确性.

表 1 准确性验证结果

| 电路 | I/O | $E_d$ | $E_s$ | 时间/s | |
|---|---|---|---|---|---|
| | | | | 算法 2 | 算法 1 |
| cm151a | 12/2 | 33.33 | 60.70 | 0.017 | 0.009 |
| cm162a | 14/5 | 51.62 | 65.46 | 0.073 | 0.012 |
| cu | 14/11 | 34.08 | 62.67 | 0.067 | 0.010 |
| pcle | 19/9 | 58.73 | 79.88 | 3.266 | 0.012 |
| sct | 19/15 | 86.21 | 171.98 | 8.988 | 0.029 |
| t3 | 12/1 | 85.87 | 346.87 | 0.167 | 0.190 |
| t481 | 16/1 | 40.22 | 61.65 | 0.296 | 0.016 |

由表 1 中的时间数据可以看出,与算法 2 相比,对于绝大多数电路,算法 1 具有更高的功耗计算时间效率. 特别是对输入数较多的电路,如 pcle 和 sct,与算法 2 相比,算法 1 将功耗计算的时间效率至少提高了 2 个数量级.

### 4.3 功耗计算方法比较

对于一组输入数大于 14 的 ITC99 和 MCNC 电路,算法 1、算法 3、算法 4 以及 ACE2.0 的功耗计算结果如表 2 所示,其中的 $E_d$ 和 $E_s$ 也分别为 100 个 MPRM 电路动态功耗以及静态功耗计算结果的平均值,$E_s$ 的单位是 μA. 其中最后一行的“总体平均”指的是实验所用 1000 个 MPRM 电路功耗计算结果的平均值.

表 2 四种算法功耗计算结果

| 电路 | I/O | 算法 1 | | 算法 3 | | 算法 4 | | ACE2.0 | |
|---|---|---|---|---|---|---|---|---|---|
| | | $E_d$ | $E_s$ | $E_d$ | $E_s$ | $E_d$ | $E_s$ | $E_d$ | $E_s$ |
| b03 | 34/34 | 276.25 | 754.18 | 345.56 | 751.88 | 276.25 | 750.29 | 276.27 | 753.16 |
| b08 | 30/25 | 174.80 | 389.33 | 200.05 | 388.51 | 174.80 | 386.09 | 174.62 | 388.84 |
| b10 | 28/23 | 214.56 | 436.07 | 265.01 | 434.31 | 214.56 | 432.67 | 214.62 | 435.18 |
| c8 | 28/18 | 107.54 | 111.99 | 118.91 | 111.54 | 107.54 | 110.96 | 107.54 | 111.64 |
| duke2 | 22/29 | 197.55 | 1743.73 | 332.32 | 1739.32 | 197.55 | 1736.68 | 197.90 | 1742.57 |
| m181 | 15/9 | 61.69 | 66.73 | 73.20 | 66.44 | 61.69 | 65.95 | 61.69 | 66.48 |
| pcler8 | 27/17 | 107.49 | 324.38 | 126.26 | 323.69 | 107.49 | 322.44 | 107.79 | 323.91 |
| pm1 | 16/13 | 35.64 | 42.59 | 45.26 | 42.42 | 35.64 | 42.18 | 35.62 | 42.42 |
| ttt2 | 24/21 | 149.24 | 325.83 | 182.09 | 324.53 | 149.24 | 323.41 | 149.31 | 325.09 |
| vda | 17/39 | 502.70 | 2858.91 | 730.08 | 2850.88 | 502.70 | 2850.51 | 502.64 | 2856.67 |
| 总体平均 | | 182.75 | 705.37 | 241.87 | 703.35 | 182.75 | 702.12 | 182.80 | 704.60 |

根据表 2 数据,分别计算算法 3、算法 4 和 ACE2.0 的平均功耗计算结果的相对误差(%),即对于每一个电路,这 3 种算法 100 个 MPRM 电路动态功耗计算结果的平均值以及静态功耗计算结果的平均值相对于算法 1 动态功耗计算结果平均值以及静态功耗计算结果平均值的误差. 结果如表 3 所示,其中最后一行的“总

体平均”是根据表 2 最后一行的“总体平均”结果计算.

**表 3　平均功耗计算结果的相对误差**

| 电路 | 算法 3 | | 算法 4 | | ACE2.0 | |
|---|---|---|---|---|---|---|
| | $E_d$ | $E_s$ | $E_d$ | $E_s$ | $E_d$ | $E_s$ |
| b03 | 25.09 | −0.30 | 0 | −0.52 | 0.01 | −0.14 |
| b08 | 14.45 | −0.21 | 0 | −0.83 | −0.10 | −0.13 |
| b10 | 23.51 | −0.40 | 0 | −0.78 | 0.03 | −0.20 |
| c8 | 10.57 | −0.40 | 0 | −0.92 | 0 | −0.31 |
| duke2 | 68.22 | −0.25 | 0 | −0.40 | 0.18 | −0.07 |
| m181 | 18.66 | −0.43 | 0 | −1.17 | 0 | −0.37 |
| pcler8 | 17.46 | −0.21 | 0 | −0.60 | 0.28 | −0.14 |
| pm1 | 26.99 | −0.40 | 0 | −0.96 | −0.06 | −0.40 |
| ttt2 | 22.01 | −0.40 | 0 | −0.74 | 0.05 | −0.23 |
| vda | 45.23 | −0.28 | 0 | −0.29 | −0.01 | −0.08 |
| 总体平均 | 32.35 | −0.29 | 0 | −0.46 | 0.03 | −0.11 |

表 3 中的相对误差为正值表示相对于算法 1 的功耗计算结果,该算法的功耗计算结果将功耗“高估”,为负值则表示该算法的功耗计算结果将功耗“低估”. 对实验所用的 1000 个 MPRM 电路做进一步分析,在这些 MPRM 电路中,算法 3 和 ACE2.0 的动态功耗计算结果和静态功耗计算结果既存在“低估”的情形,也存在“高估”的情形,算法 4 动态功耗计算结果的相对误差均为 0,静态功耗计算结果均为“低估”. 关于表 3 中的电路 c8 和 m181,ACE2.0 的平均动态功耗计算结果的相对误差为 0,只是说明这两个电路,其 100 个 MPRM 电路动态功耗计算结果的“高估”部分和“低估”部分恰好相互抵消.

表 4 则给出了算法 3、算法 4 和 ACE2.0 针对每一个电路,其 100 个 MPRM 电路功耗计算结果的最大相对误差(%),即相对于算法 1 功耗计算结果的最大误差,在统计最大相对误差时,如相对误差为负值则取其绝对值.

**表 4　功耗计算结果的最大相对误差**

| 电路 | 算法 3 | | 算法 4 | | ACE2.0 | |
|---|---|---|---|---|---|---|
| | $E_d$ | $E_s$ | $E_d$ | $E_s$ | $E_d$ | $E_s$ |
| b03 | 63.84 | 0.88 | 0 | 0.74 | 2.30 | 0.38 |
| b08 | 55.07 | 0.58 | 0 | 1.30 | 3.44 | 0.34 |
| b10 | 66.46 | 1.04 | 0 | 1.10 | 1.47 | 0.50 |
| c8 | 26.90 | 0.92 | 0 | 1.18 | 1.22 | 0.80 |
| duke2 | 155.64 | 0.80 | 0 | 0.59 | 3.64 | 0.20 |
| m181 | 41.74 | 1.26 | 0 | 1.35 | 2.22 | 0.80 |
| pcler8 | 71.37 | 0.38 | 0 | 1.10 | 3.51 | 0.65 |
| pm1 | 63.58 | 1.14 | 0 | 1.19 | 2.53 | 0.85 |
| ttt2 | 84.62 | 0.79 | 0 | 1.14 | 2.22 | 0.51 |
| vda | 143.16 | 0.84 | 0 | 0.52 | 2.53 | 0.35 |

表 3 和表 4 中算法 3 动态功耗计算结果相对误差的大小反映了 MPRM 电路中信号间相关性的强弱,即反映了定义 1 中的 $T_u$ 和 $T_w$ 之间关于 PI 信号相关性的强弱,相关性越强,忽略相关性所导致的动态功耗计算结果的相对误差也越大;另外,如果 XOR 部分的动态功耗占电路总体动态功耗的比例越大,那么相关性的忽略所导致的动态功耗计算结果的相对误差也相对越大. 算法 4 中的 BDD 信号概率计算方法能够得到准确的 $\mathrm{Pr}(g_k)$ 计算结果,因此也能够得到准确的动态功耗计算结果. ACE2.0 中计算信号概率的 BDD 符号模拟法采用的是伪随机符号模拟,根据 PI 的信号概率生成的伪随机输入向量可以使 $\mathrm{Pr}(g_k)$ 的误差被控制在一个较小的范围之内,因此其动态功耗计算结果的相对误差较小.

算法 4 中计算信号概率的 BDD 法在计算 $P_{k,v}=\mathrm{Pr}(\tilde{s}_{k,1}\tilde{s}_{k,2})$ 时没能够很好地解决 $\tilde{s}_{k,1}$ 和 $\tilde{s}_{k,2}$ 间的相关性. 由于仅 XOR 部分中的异或门的信号间存在相关性,因此静态功耗计算结果误差的大小与异或门 $g_k$ 的输入信号 $\tilde{s}_{k,1}$ 和 $\tilde{s}_{k,2}$ 间相关性的强弱有关,相关性越强,$P_{k,v}$ 计算结果的误差也越大,静态功耗计算结果的误差也越大. 由于信号 $x_i$ 与 $\bar{x}_i$ 互斥,当 $x_i\in s_{k,1}\wedge x_i\in s_{k,2}$ 或者 $\bar{x}_i\in s_{k,1}\wedge\bar{x}_i\in s_{k,2}$ 时,可以认为 $\bar{s}_{k,1}$ 与 $s_{k,2}$ 以及 $s_{k,1}$ 与 $\bar{s}_{k,2}$ 不存在关于 $x_i$ 的相关性;当 $\bar{x}_i\in s_{k,1}\wedge x_i\in s_{k,2}$ 或者 $x_i\in s_{k,1}\wedge\bar{x}_i\in s_{k,2}$ 时,可以认为 $s_{k,1}$ 与 $s_{k,2}$ 以及 $\bar{s}_{k,1}$ 与 $\bar{s}_{k,2}$ 不存在关于 $x_i$ 的相关性,正因为如此,使得异或门 $g_k$ 的输入信号 $\tilde{s}_{k,1}$ 和 $\tilde{s}_{k,2}$ 关于 PI 信号的相关性较弱甚至可能相互独立,从而使得算法 4 计算 $P_{k,v}$ 的误差减小,也使得其静态功耗计算结果的相对误差较小.

算法 3 和 ACE2.0 采用了 $P_{k,v}=\mathrm{Pr}(\tilde{s}_{k,1})\times\mathrm{Pr}(\tilde{s}_{k,2})$ 的方法计算 $P_{k,v}$,也正是因为如上所述原因,使得算法 3 和 ACE2.0 的静态功耗计算结果的相对误差也较小.

表 5 给出了算法 1、算法 3、算法 4 和 ACE2.0 的功耗计算时间(100 个 MPRM 电路功耗计算时间的平均值),单位为秒.

**表 5　四种算法的功耗计算时间**

| 电路 | 算法 1 | 算法 3 | 算法 4 | ACE2.0 |
|---|---|---|---|---|
| b03 | 0.239 | <0.001 | 0.064 | 1.150 |
| b08 | 0.105 | <0.001 | 0.033 | 0.668 |
| b10 | 0.098 | <0.001 | 0.032 | 0.749 |
| c8 | 0.023 | <0.001 | 0.009 | 0.229 |
| duke2 | 0.679 | <0.001 | 0.171 | 2.847 |
| m181 | 0.012 | <0.001 | 0.004 | 0.129 |
| pcler8 | 0.059 | <0.001 | 0.029 | 0.525 |
| pm1 | 0.003 | <0.001 | 0.002 | 0.085 |
| ttt2 | 0.055 | <0.001 | 0.023 | 0.511 |
| vda | 2.362 | <0.001 | 0.285 | 4.860 |
| 平均 | 0.364 | <0.001 | 0.065 | 1.175 |

由表 5 可以看出,算法 3 功耗计算的时间效率最高,ACE2.0 因采用了 BDD 符号模拟法计算信号概率,功耗计算的时间效率最低,算法 1 功耗计算的时间效率要低于算法 4.

综合以上数据可以看出,与算法 3 相比,算法 1 能够提高动态功耗和静态功耗计算结果的准确度,算法 1 将动态功耗计算结果的准确度最大提高了 155.64%,将总体平均动态功耗计算结果的准确度提高了 32.35%,同时算法 1 将静态功耗计算结果的准确度最大提高了 1.26%,将总体平均静态功耗计算结果的准确度提高了 0.29%. 算法 1 和算法 4 均能得到准确的动态功耗计算结果,与算法 4 相比,算法 1 将静态功耗计算结果的准确度最大提高了 1.35%,将总体平均静态功耗计算结果的准确度提高了 0.46%. 尽管从总体平均动态功耗计算结果的角度看,ACE2.0 相对于算法 1 的误差(0.03%)可以忽略,但与 ACE2.0 相比,算法 1 将动态功耗计算结果的准确度最大提高了 3.64%,同时算法 1 将静态功耗计算结果的准确度最大提高了 0.85%,将总体平均静态功耗计算结果的准确度提高了 0.11%,并将时间效率提高了 69.02%.

综上所述,当采用基于信号概率的功耗计算模型进行 MPRM 电路的功耗计算时,本文所提出的基于概率表达式的 MPRM 电路功耗计算方法能够在合理的时间内获得准确的电路功耗计算结果.

## 5 结语

随着芯片制造工艺的发展,已无法再通过缩小晶体管尺寸进一步降低功耗,再加上芯片复杂度的上升,如不解决功耗问题,芯片中大量晶体管所产生的热量将达到晶体管所能够承受的极限,内部过热将严重影响芯片的可靠性甚至导致芯片的损坏从而引起系统的失效,这使得 RM 电路的功耗优化成为一个非常重要的现实问题. 在采用基于信号概率的功耗计算模型进行 RM 电路的功耗优化时,需要解决电路中信号间的空间相关性问题. 提出了一种基于概率表达式的 MPRM 电路功耗计算方法,利用概率表达式计算信号概率来解决电路中信号间的空间相关性问题,并使用二元矩图表示概率表达式. 基准电路的实验结果表明所提出方法准确有效.

### 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] WANG X, LIU Y, ZHANG Y, et al. Power optimization in logic synthesis for mixed polarity Reed-Muller logic circuits[J]. The Computer Journal, 2015, 58(6): 1306 – 1313.

[5] WANG P, LI K, ZHANG H. PMGA and its application in area and power optimization for ternary FPRM circuit[J]. Journal of Semiconductors, 2016, 37(1): 126 – 130.

[6] DAS A, PRADHAN S N. Shared Reed-Muller decision diagram based thermal-aware AND-XOR decomposition of logic circuits[J]. VLSI Design, 2016, 2016: 3191286: 1 – 3191286: 14.

[7] 俞海珍,汪鹏君,张会红,等. 基于三值多样性粒子群算法的 MPRM 电路综合优化[J]. 电子学报, 2017, 45(7): 1601 – 1607.
YU Hai-Zhen, WANG Peng-Jun, ZHANG Hui-Hong, et al. Optimization of MPRM circuits based on ternary diversity particle swarm optimization[J]. Acta Electronica Sinica, 2017, 45(7): 1601 – 1607. (in Chinese)

[8] HE Z-X, XIAO L-M, RUAN L, et al. A power and area optimization approach of mixed polarity Reed-Muller expression for incompletely specified Boolean functions[J]. Journal of Computer Science and Technology, 2017, 32(2): 297 – 311.

[9] DUNOYER J, ABDALLAH N, SABET P B. A symbolic simulation approach in resolving signals´ correlation[A]. Proceedings of the 29th Annual Simulation Symposium[C]. New Orleans, LA, USA: IEEE Press, 1996. 203 – 211.

[10] PARKER K P, MCCLUSKEY E J. Probabilistic treatment of general combinational networks[J]. IEEE Transactions on Computers, 1975, C – 24(6): 668 – 670.

[11] KUMAR S K, BREUER M A. Probabilistic aspects of Boolean switching functions via a new transform[J]. Journal of ACM, 1981, 28(3): 502 – 520.

[12] BRYANT R E, CHEN Y-A. Verification of arithmetic circuits using binary moment diagrams[J]. International Journal on Software Tools for Technology Transfer, 2001, 3(2): 137 – 155.

[13] ABBAS Z, OLIVIERI M. Impact of technology scaling on leakage power in nano-scale bulk CMOS digital standard

cells[J]. Microelectronics Journal, 2014, 45(2): 179 – 195.

[14] LUO H, NOURANI M. Aging and leakage tradeoff in VLSI circuits[A]. Proceedings of the 10th International Design & Test Symposium[C]. Amman, Jordan: IEEE Press, 2015. 106 – 111.

[15] 卜登立,江建慧. 基于 Pareto 支配的 MPRM 电路面积与可靠性优化[J]. 电子学报, 2016, 44(11): 2653 – 2659.
BU Deng-li, JIANG Jian-hui. Pareto dominance based area and reliability optimization of MPRM circuits[J]. Acta Electronica Sinica, 2016, 44(11): 2653 – 2659. (in Chinese)

[16] LAMOUREUX J. ACE2.0-a Probabilistic Activity Estimation Tool[DB/OL]. http://www.ece.ubc.ca/~julienl/activity.htm. 2014 – 08 – 05.

[17] YANG S. Logic Synthesis and Optimization Benchmarks User Guide, Version 3.0[R]. North Carolina: Microelectronics Center of North Carolina, 1991.

## 作者简介

**卜登立** 男,1975 年出生,河北定州人. 博士,副教授,中国电子学会高级会员,主要研究领域为电路设计与优化、可逆逻辑综合、量子电路综合、启发式优化算法.
E-mail: bodengli@163.com