

文章编号:1005-0523(2014)06-0087-06

基于SAT的可逆线路检测集生成算法

李明翠,周日贵

(华东交通大学信息学院,江西 南昌 330013)

摘要:可逆逻辑是量子计算的基本特征,也是日益突出的低能耗需求的一种解决方案。根据可逆电路的可控制性和可观测性,论文提出了一种基于逻辑可满足性的算法来自动产生单门失效错误的完备检测集。基于 k -NOT门的可逆逻辑线路中的数据传送进行线性建模,用线性时态逻辑描述单门失效错误约束,运用SAT求解器寻求反例的方法自动生成可逆电路的错误检测集。实验结果显示,本方法能够有效的应用于不规则和复杂的基于 k -NOT门的可逆逻辑线路,自动化程度高。

关键词:可逆;量子;SAT;门失效;错误检测

中图分类号:TP387;TP306+.2

文献标志码:A

能耗和散热是电子产品功能越来越复杂、体积越来越小发展过程中日益突出的问题。由于可逆线路的低能耗特性,可逆线路被认为未来量子计算、纳米技术以及低功耗COMS等领域的一种解决方案。计算机每擦除一位信息就会释放至少 $kT \ln 2$ J 的热量 (k 是波尔兹曼常数 1.38×10^{-23} , T 是计算时的绝对温度)^[1]。不可逆电路中的能量消耗与在计算过程中擦除的信息位数成正比。而可逆线路要求在计算过程中保持输入和输出的一一对应关系,因此可逆计算没有信息丢失。Bennett^[2]指出如果所有的运算都是用可逆部件完成的话,零能耗将成为可能。Barenco等^[3]指出任何的运算在逻辑上和热力学上都可以以可逆的方式进行。另一方面,由于量子物理学中的酉变换是可逆的,因此,可逆线路是量子力学中的最基本部分。从可逆门的设计到加法器及各种可逆电路的合成,国内外学者进行了很多相关的研究^[4-7]。为了保证电路的正确性,在电路设计过程中和设计后的错误检测非常重要。可逆电路的错误模型和检测集生成方法与传统电路存在很大的不同。目前提出的可逆线路错误模型主要有:固定点错误模型、单门失效模型、门重复错误模型、多门失效错误模型、门部分控制点失效等模型。Patel^[8]提出的错误检测集产生方法(ILP),Ramasamy^[9]提出的基于错误表的适应树方法,以及文献^[10-13]设计的基于奇偶保持的可逆容错线路,都是针对可逆电路的固定点错误模型。然而,在可逆线路中,更能体现整个电路是否实现了目标功能的是门错误模型。Polian等人^[14]用离子阱技术通过激光脉冲作用于离子的方式模拟了基于 k -NOT门的可逆电路的单门失效(SMGF)、门重复(RGF)、连续位置的多门失效(MMGF和门部分失效(PMGF)错误模型。Hayes等^[15]提出了基于 k -NOT门的门失效错误模型(MGF)检测方法DFT。DFT方法是在原有线路中增加一条传输线和多个受控非门,这种方法的优点是仅用一个检测向量就能检测整个线路中是否存在单个门错误,但其缺点也很明显:为了辅助错误检测而增加的多个受控非门本身也可能产生新的错误,这些门一旦产生错误,DFT方法的优点将不复存在。肖芳英等人^[16]提出了根据门间占据关系检测单门失效的错误完备测试集算法

收稿日期:2014-09-19

基金项目:国家自然科学基金项目(61340029,61462026);江西省教育厅青年科学基金项目(GJJ14395);江西省科技厅对外科技合作项目(20141BDH80007);江西省教育厅科技项目(KJLD14037)

作者简介:李明翠(1980—),女,讲师,硕士,研究方向为可逆量子逻辑线路的合成与检测;周日贵(1973—),男,教授,博士,研究方向为量子信息。

CTS,这种方法不适于复杂的不规则电路。Zhang^[17]提出了用向量反复迭代的方式获得单门失效最小测试集的方法,其缺点是每生成一个测试向量都要用该向量对剩余错误进行迭代检测。Kole^[18]提出了连续位置门失效问题测试集的生成算法。以下根据SAT可满足性原理着重研究基于 k -NOT门的可逆电路的单门失效错误检测集的自动产生方法。

1 可逆电路中的单门失效错误模型

可逆电路的输入和输出具有一一对应的双射关系, n 位输入的可逆电路必有 n 位输出,常用 $n \times n$ 表示具有 n 位输入和 n 位输出的可逆电路。一个 $n \times n$ 的可逆电路的真值表具共有 2^n 行输入和 2^n 行输出。对于基本的二进制位输入,可逆电路的输出是输入的某个排列置换。可逆电路从左到右对信息进行线性转换,每向右边增加一次转换称为深度增加1。 k -NOT门是组成可逆电路的最常用基本门。一个 k -NOT门有 k 个控制位 $c_1, c_2, \dots, c_k$ 和一个目标位 t ,实现的是一个 $(k+1) \times (k+1)$ 的西变换。 k -NOT门的逻辑功能为 $|c_1, c_2, \dots, c_k, t\rangle \rightarrow |c_1, c_2, \dots, c_k, t \oplus (c_1 c_2 \dots c_k)\rangle$,即控制位的输入与输出相同,当所有的控制位的输入都为1时,目标位的输出与输入相反。其中0-NOT相当于一个反向器(NOT),输出与输入相反,1-NOT也叫控制非门(CNOT),2-NOT门也叫Toffoli门。图1描述了这三种门的逻辑表示方式,其中门的控制位用 $\cdot$ 表示,目标位用 $\oplus$ 表示。

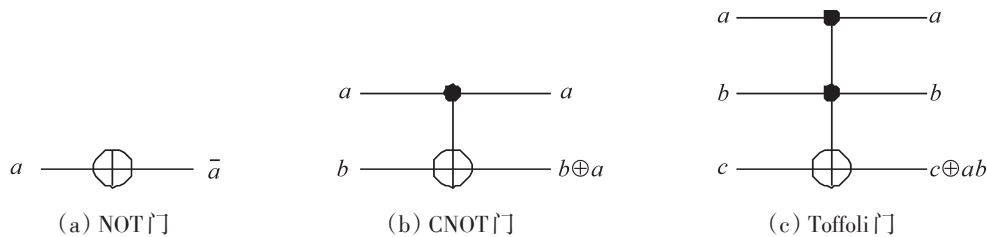


图1 三种基本可逆门

Fig.1 Three elementary reversible gates

单门失效错误(SMGF)指的是电路中的一个 k -NOT门的功能完全消失,其所在位置相当于传输线直接连通的效果。实现该门的激光脉冲太短或者消失或没有调整到位都可能是造成SMGF的物理原因。可逆线路具有非可逆线路所没有的两个重要特征可控制性和可观测性。可控制性是指,存在一个检测向量能产生电路中任意指定位置所需要的状态,即在电路的某个深度指定的任意状态都有一个对应的输入向量。可观察性指任何一个改变某个中间状态的错误也同时改变输出。根据可控性和可观测性,一个SMGF可以通过设置失效门的所有控制点输入为1,其他输入是0或1来检测。图2(电路来源于可逆电路测试网站 <http://www.cs.uvic.ca/~dmaslov>)描述了虚线框中的2-NOT门失效的SMGF错误。在图2的例子中,如果输入 $\{in1, in2, in3\} = \{0, 1, 1\}$,正确的输出应该是 $\{out1, out2, out3\} = \{1, 0, 0\}$,然而,当虚线框中的SMGF发生后输出变成了 $\{out1, out2, out3\} = \{0, 1, 1\}$ 。线路中可能的SMGF数量与线路中门的数量相等。

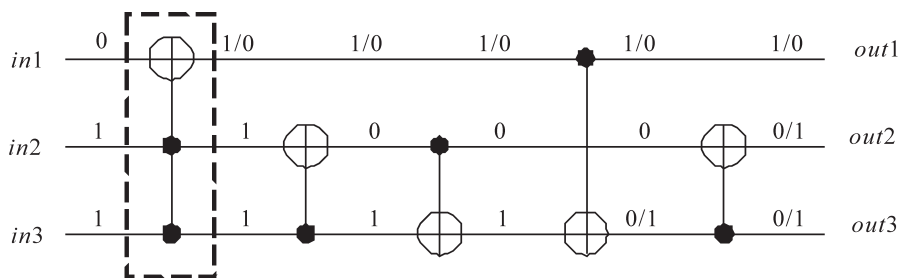


图2 单门失效错误(SMGF)

Fig.2 Single missing-gate fault (SMGF)

2 基于SAT的单门失效错误完备检测集生成算法

布尔可满足性问题 (SAT)是指对给定的一个包含 k 个布尔变量的逻辑函数 h , 确定是否存在这 n 个变量的一组取值组合, 使得 h 的值为1或者证明不存在使得 h 为1的取值组合。如果赋值组合存在则称为可满足 (SAT), 否则, 称为不可满足 (UNSAT)。SAT问题是计算机理论界和逻辑学界共同关注的重大问题, 被广泛的应用于自动规划、模型诊断和电路等价性等方面的研究。SMGF问题可以转化为这样一个SAT问题“是否存在这样一个输入向量, 使得 k -NOT 门 g_j 的所有控制位输入为1, $1 \leq j \leq m$, m 是线路中的 k -NOT 总数”。用NuSMV模型检测器检测指定的可逆线路是否满足某个线性属性。

2.1 可逆线路中的数据传输建模

给定一个具有 n 条传输线和 m 个 k -NOT 门的可逆线路。假定所有的初始输入为基本的二进制输入0和1, 则 n 位的0和1的组合沿着传输线从左到右依次经过 m 个可逆门进行传输和转化。将电路中的 n 位数据用向量 $A = a_1 a_2 \cdots a_n$ 表示, A 每经过一个 k -NOT 门, 状态会发生改变, 我们用 a_i^j 表示第 i 位数据经过第 j 个门后的状态, 用 g_j 表示第 j 个门, $1 \leq i \leq n$, $1 \leq j \leq m$ 。则 a_i^j 的转化可以用数学公式(1)描述。公式(1)表示 n 位信息经过 g_j 后, 只有 g_j 的目标位所在的传输线中的信息会发生变化, 其余信息位不变。

$$a_i^{j+1} = \begin{cases} a_i^j, & \text{可逆门 } g_{j+1} \text{ 的目标位不在第 } i \text{ 条传输线上} \\ a_i^j \oplus \bigwedge a_c^j, & \text{可逆门 } g_{j+1} \text{ 的目标位在第 } i \text{ 条传输线上, } a_c^j \text{ 是 } g_{j+1} \text{ 的所有控制位输入集合} \end{cases} \quad (1)$$

例如图3中可逆线路Ham3中的信息转化关系为

$$\begin{cases} a_1^1 = a_1^0 \oplus a_2^0 a_3^0 & a_2^1 = a_2^0 & a_3^1 = a_3^0 \\ a_1^2 = a_1^1 & a_2^2 = a_2^1 \oplus a_3^1 & a_3^2 = a_3^1 \\ \dots & & \\ a_1^5 = a_1^4 & a_2^5 = a_2^4 \oplus a_3^4 & a_3^5 = a_3^4 \end{cases} \quad (2)$$

图3 Ham3中的信息传输

Fig.3 Data transformation in reversible circuit Ham3

2.2 SMGF 错误约束

m 个 k -NOT 门组成的可逆线路有 m 个可能的SMGF错误。根据线路中门的输入输出关系, 将 m 个可逆门生成 m 个数据转化实例 $gc_1, gc_2, \dots, gc_m$ 。这 m 个实例的数据输入输出关系用公式(3)描述, 其中 $gc_{j+1}.in[i]$, 是第 $j+1$ ($1 \leq j \leq m-1$, $1 \leq i \leq n$) 个层次(深度)的输入向量, $gc_j.out[i]$ 是经过第 j 个层次的 k -NOT 门后得到的输出。

$$\begin{cases} gc_{j+1}.in[1] = gc_j.out[1] \\ gc_{j+1}.in[2] = gc_j.out[2] \\ \dots \\ gc_{j+1}.in[n] = gc_j.out[n] \end{cases} \quad (3)$$

一个SMGF的错误检测可以约束为将该失效门的所有控制点输入为设置为1。例如图3中的编号为2的CNOT门的错误检测约束为 $a_3^1 = 1$, 即 $gc_1.out[3] = 1$ 。同理编号为4的CNOT门的错误检测约束为 $a_1^3 = 1$, 即 $gc_3.out[1] = 1$ 。公式(4)用线性时态逻辑(LTL)描述了第 $j+1$ 个 k -NOT 门的错误约束的反, 用来表示指定

线路不存在满足指定公式的属性,其中 $p, q, \dots, r \in C_{j+1}$, C_{j+1} 是第 $j+1$ 个 k -NOT 门的控制点集合。

$$!F(gc_j.out[p]=1 \& gc_j.out[q]=1 \& \dots \& gc_j.out[r]=1) \quad (4)$$

根据公式(4),图3的Ham3线路中5个单门失效错误约束取反可以描述如下

$$\left\{ \begin{array}{l} !F(gc0.b[2]=1 \& gc0.b[3]=1) \\ !F(gc1.b[3]=1) \\ !F(gc2.b[2]=1) \\ !F(gc3.b[1]=1) \\ !F(gc4.b[3]=1) \end{array} \right. \quad (5)$$

将数据传输模型和错误约束 LTL 公式输入 SAT 检测器 NuSMV,得到的反例就是每个错误的输入检测向量。Ham3 根据公式(1)~(5)得到的一组检测集向量为(011, 111, 101, 011, 101),合并后得到(011, 111, 101),因此(011, 111, 101)是图3所示Ham3的SMGF完备检测集。

3 实验结果分析

可逆线路单门失效错误检测集生成算法实验结果如表1所示。

表1 文章所提出方法的实验结果

Tab.1 Experiment results of the proposed method

可逆电路	传输线 n	可逆门 m	检测集大小	完备检测集
Ham3	3	5	3	{3,5,7}
4b15g_1	4	15	7	{6,1,15,5,8,3,10}
Mod5d1	5	8	1	{31}
5bitadder	11	29	19	{1706,1571,989,1906,1901,1843,1910,1209,745, 685,1737, 494,1242,1591,1483,1585,1484,1704,683}
Gf2^4mult	12	19	10	{4000,3888,3440,4048,944,4064,4080,4016,3952, 3568}
Cycle17_3	20	48	25	{1048567,1048543,1048511,786431,786303, 1048559, 1048319,1048565,1048569,262143, 520191,1015807, 1048575,917499,1048570, 393215,1048566, 917495, 917503, 786430,655359, 1048572, 917501, 655351, 1048574 }
Mod1024adder	20	55	41	1048543,1048573,1048559,1048323,1048521, 1048571, 1048463,1048561,1048562,1048535, 1048574,1048481, 1048483,1048550,1048495, 1048383,1048129,1048386, 1048515,1048133, 1048158,1048575,1048320,1048192, 1048451, 1048196,1048199,1048223,1048239,1048322, 1048335,1048351,1048353,1048391,1048064, 1048066, 1048071,1048072,1048095,1048128, 1048255

实验所用线路全部来自可逆线路测试网站(<http://www.cs.uvic.ca/~dmaslov>)。表中第1列是所选用的可逆线路名称,第2列是线路的传输线数目,第3列是线路中包含的可逆门数目,第4列是用本文提出的方法得到的完备检测集大小,第五列是具体的检测集,其中所有的检测向量都已转换为十进制数,其对应的二进制数从高位到低位对应于线路的传输线1,2,..., n 的输入。实验结果显示本方法对于无规则线路和复杂线路均有效。

在检测过程中,由于NOT门可以被任意输入向量检测到,因此在检测集生成时可以忽略NOT门的检测向量生成。对输入有特殊限制的电路(例如Mod5d1的最后一根输入线要求是1, Gf2^4mult的最后四根线

的输入要求为常量0), 可以将错误约束 LTL 公式进行特征约束扩展, 将公式(4)扩展成公式(6), 其中 $a0$ 是电路最左端的初始输入, $u, \dots, v \in \{1, 2, 3, \dots, n\}$ 是对输入有特殊限制的传输线编号, w 根据具体线路的输入限制取0或1。

$$! F (a0[u]=w \& \dots \& a0[v]=w \& gc_i.out[p]=1 \& gc_i.out[q]=1 \& \dots \& gc_i.out[r]=1) \quad (6)$$

4 总结

可逆线路的可控制性保证了可以求得任意指定层次数据对应的原始输入向量, 可观测性保证了任意层次数据的改变将直接反应到输出结果。根据可控性和可观测性, 将检测向量生成问题转化为求解逻辑可满足问题, 通过在 k -NOT 门的对应层次上指定其所有控制位输入为1的约束条件来获得对应的检测向量。将逻辑线路的数据转化抽象成线性逻辑公式, 用线性时态逻辑 LTL 描述所求问题的反, 通过求反例的方式来自动生成整个可逆电路的完备单门失效错误检测集。用可逆线路网站上的部分线路检测提出的方法, 实验结果显示此方法能够很好的产生完备检测集, 自动化程度高, 能应对不规则的复杂线路, 易于针对线路的特殊属性进行扩展。

参考文献:

- [1] LANDAUER R. Irreversibility and heat generation in the computing process[J]. IBM Journal of Research and Development, 1961, 5(3):183-191.
- [2] BENNETT C H. Logical reversibility of computation[J]. IBM journal of Research and Development, 1973, 17(6):525-532.
- [3] BARENCO A, BENNETT CH, CLEVE R. Elementary gates for quantum computation[J]. Canadian Metallurgical Quarterly, 1995, 52(5):3457-3467.
- [4] TOFFOLI T. Reversible computing[M]. Berlin Heidelberg:Springer, 1980:1-34.
- [5] THAPLIYAL H, SRINIVAS M B. A novel reversible TSG gate and its application for designing reversible carry look-ahead and other adder architectures[M]. Berlin Heidelberg: Springer, 2005:805-817.
- [6] 黎海生, 周日贵. 在纠缠量子系统中的图像几何形状存储和检索[J]. 华东交通大学学报, 2013, 30(4):14-18.
- [7] ZHOU RIGUI, ZHANG MAN QUN, WU QIAN, et al. Optimization approaches for designing a novel 4-bit reversible comparator [J]. International Journal of Theoretical Physics, 2013, 52(2):559-575.
- [8] PATEL K N, HAYES J P, MARKOV I L. Fault testing for reversible circuits[J]. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 2004, 23(8):1220-1230.
- [9] RAMASAMY K, TAGARE R, PERKINS E, et al. Fault localization in reversible circuits is easier than for classical circuits[C]// Proceedings of the International Workshop on Logic and Synthesis, June 2004.
- [10] SAFARI P, HAGHPARAST M, AZARI A, et al. A design of fault tolerant reversible arithmetic logic unit[J]. Life Science Journal, 2012, 9(3):643-646.
- [11] BOROUHAND S, HAGHPARAST M. A novel nanometric fault tolerant reversible associative memory cell[J]. Australian Journal of Basic and Applied Sciences, 2011, 5(10):945-950.
- [12] MITRA S K, CHOWDHURY A R. Minimum cost fault tolerant adder circuits in reversible logic synthesis[C]//VLSI Design (VL-SID), 2012 25th International Conference. IEEE, 2012:334-339.
- [13] ZHOU R G, LI Y C, ZHANG M Q. Novel designs for fault tolerant reversible binary coded decimal adders[J]. International Journal of Electronics, 2014, 101(10):1336-1356.
- [14] POLIAN I, FIEHN T, BECKER B, et al. A family of logical fault models for reversible circuits[C]//Test Symposium, 2005 Proceedings 14th Asian. IEEE, 2005:422-427.

- [15] HAYES J P, POLIAN I, BECKER B. Testing for missing-gate faults in reversible circuits[C]//Test Symposium, 2004 13th Asian. IEEE, 2004:100–105.
- [16] 肖芳英,陈汉武,李志强. 量子电路中门失效错误的检测方法[J]. 仪器仪表学报, 2008,29(10):2084–2089.
- [17] ZHANG H, FREHSE S, WILLE R, et al. Determining minimal testsets for reversible circuits using boolean satisfiability[C]//Afri-con. IEEE, 2011:1–6.
- [18] KOLE D K, RAHAMAN H, DAS D K, et al. Derivation of test set for detecting multiple missing-gate faults in reversible circuits [J]. Computers and Electrical Engineering, 2013,39(2):225–236.

SAT-based Algorithm for Generating Test Set of Reversible Circuits

Li Mingcui,Zhou Rigui

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: Reversible logic is the basic feature of quantum computing, and is also a solution to the increasingly prominent low energy demand. According to the controllability and observability of reversible circuits, this paper presents a novel algorithm which is based on the logic satisfiability to generate the complete test set automatically for single missing-gate fault in reversible circuits. The data transmissions of reversible logic circuits based on $k- NOT$ gates are linear modeled, and the constraint of single missing-gate faults are described by linear temporal logic. The test sets are generated automatically by applying the circuit models and the fault constraints to the SAT solver to obtain the counterexample. Experimental results show that this method can generate test set effectively with high degree of automation for irregular and complex reversible logic circuit based on $k- NOT$ gates.

Key words: reversible; quantum; SAT; gate fault; fault detection