具有故障定位能力的健壮故障安全系统

江建慧[1,2],施鸿宝[1]
(1 上海铁道大学计算技术研究所,上海 200331;2 中国科学院计算技术研究所 CAD 开放研究实验室,北京 100080)

摘 要: 本文以广义故障安全系统理论、数字电路的并发差错定位概念为基础,提出了一种健壮故障安全系统理论.一个基本健壮故障安全电路是由一个实现电路基本功能的基本功能电路和一个差错定位转换器所组成的.健壮故障安全电路具有并发差错定位能力.文中定义了表征健壮故障安全电路和差错定位转换器的基本特性;证明了基本功能电路与差错定位转换器互连,以构造几种具有不同健壮故障安全特性的基本电路所需满足的条件;最后还用电路实例说明了该理论的应用.

关键词: 故障安全; 健壮故障安全; 并发差错定位; 差错定位转换器; 电路互连
中图分类号: TP302 **文献标识码**: A **文章编号**: 0372-2112 (2000) 08-0035-04

Robust Fail-safe Systems with Fault Location Capability

JIANG Jian-hui[1,2], SHI Hong-bao[1]
(1. *Institute of Computing Technology, Shanghai Tiedao University, Shanghai* 200331, *China*;
2. *CAD Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: On the basis of the generalized fail-safe systems theory and the concurrent error location concept, a new theory of robust fail-safe systems is proposed. A basic robust fail-safe circuit is composed of a basic functional module and an error-locating translator. Such a circuit has concurrent error location capability. Several properties to characterize robust fail-safe circuits are defined. The interconnection conditions, which basic functional modules and translators must satisfy to construct basic circuits with different robust fail-safe properties, are proved. The usefulness of the theory is discussed along with an example of partially robust fail-safe circuits.

Key words: fail-safe; robust fail-safe; concurrent error location; error-locating translator; circuit interconnection

1 引言

故障安全电路在出现内部故障时可能产生错误的输出(属于安全值),但由于电路不具有故障自测试能力,因此,累积的故障最终将致使电路失去故障安全特性[3,6].故障安全系统理论与并发差错检测系统理论的结合形成了广义故障安全系统理论,这种广义故障安全电路具有故障自测试能力,能有效地提高电路的 MTTF 值[7,9,10].但是,当检测出故障后,要定位故障,并且将发生永久性故障的模块替换掉,则有一定的困难.系统将不得不中断正常的服务,先施加所有的测试码,查故障字典,确定故障模块与故障的性质,再进行相应的修理.如果使故障安全电路具有并发差错定位能力,即在正常工作条件下,无需任何外加用于定位故障的输入就能自动定位其内部的故障,那么,故障诊断过程就可大大加快,进一步提高了系统的维护性.因此,故障安全技术与并发差错定位技术的结合,将使电路在内部产生故障时,其功能输出保持正确或安全,同时还给出相应的差错(故障)定位信息.本文将该技术的有关概念、结构和方法称为健壮故障安全系统理论.

2 电路模型、故障模型与故障定位

一个实现函数 G 的基本健壮故障安全数字电路(以下简称基本电路)是由一个实现函数 Ω 的基本功能电路和一个实现函数 Θ_{sl} 的差错定位转换器(以下简称转换器)相互级联所构成.基本电路是构造健壮故障安全系统的基本单元.设 $N(\geq 2)$ 为基本电路中所包含的物理模块数(其大小依具体划分而定),其中,基本功能电路含有 $M(\geq 1)$ 个模块,转换器含有 $N-M(N>M)$ 个模块.

设基本电路的原始输入 X、原始输出 Y 和基本功能电路的输出 W 分别取自基本电路的完全输入集 $S(X^m)$、完全输出集 $S(Y^n)$ 和基本功能电路的完全输出集 $S(W^w)$,它们的长度分别为 m、n 和 w. Y 矢量可被分割为两部分 (Z, E),其中,Z 为电路的功能输出,E 为电路内部出错模块定位指示输出,它们分别取自基本电路的完全功能输出集 $S(Z^u)$ 和差错定位指示输出集 $S(E^v)$,矢量长度分别为 u 和 v, $u+v=n$.从语义角度考虑,可把 $S(Z^u)$ 划分为合法功能输出集 $S_n(Z^u)$ 和非法功能输出集 $S_a(Z^u)$ 两个互不相交的子集,其中 $S_n(Z^u)=S_{sn}(Z^u)$

收稿日期:1999-03-09;修回日期:1999-09-20
基金项目:国家自然科学基金(No. 69733010);上海高等学校青年教师学术基金;中国科学院计算所 CAD 开放研究实验室开放课题

$\cup S_{dn}(Z^u)$, $S_{sn}(Z^u)$ 和 $S_{dn}(Z^u)$ 分别被称为安全合法功能输出集和危险合法功能输出集. $S(E^v)$ 也可作如下划分 $S(E^v) = S_n(E^v) \cup S_l(E^v) \cup S_d(E^v)$, 其中, $S_n(E^v)$ 是电路无差错指示集, $S_l(E^v)$ 是电路产生可定位差错的差错定位指示集, $S_d(E^v)$ 是电路出现差错的差错检测指示集. 由于 $S(Y^n) = S(Z^u) \times S(E^v)$, 上述子集的组合可生成如下集合:

$$S_{sn}(Y^n) = \{(Z, E) \mid Z \in S_{sn}(Z^u) \wedge E \in S_n(E^v)\},$$

$$S_{dn}(Y^n) = \{(Z, E) \mid Z \in S_{dn}(Z^u) \wedge E \in S_n(E^v)\},$$

$$S_l(Y^n) = \{(Z, E) \mid Z \in S_{sn}(Z^u) \cup S_a(Z^u) \wedge E \in S_l(E^v)\},$$

$$S_d(Y^n) = \{(Z, E) \mid Z \in S_{sn}(Z^u) \cup S_a(Z^u) \wedge E \in S_d(E^v)\},$$

$$S_u(Y^n) = \{(Z, E) \mid Z \in S_{dn}(Z^u) \wedge (E \in S_l(E^v) \vee E \in S_d(E^v)) \vee Z \in S_a(Z^u) \wedge E \in S_n(E^v)\}.$$

其中, $S_u(Y^n)$ 表示未定义输出集, 其它集合的意义是明显的. $S_l(Y^n)$ 还可被划分为 N 个子集: $S_l(Y^n) = \cup_{i=1}^{N} S_{li}(Y^n)$, 其中, $S_{li}(Y^n) \cap S_{lj}(Y^n) = \Phi, i \neq j$, Φ 表示空集. 第 i 个 $S_{li}(Y^n)$ 是对应于第 i 个物理模块 M_i ($i = 1, 2, \cdots, N$) 出现故障时的输出集合. 因此, 我们有

$$S(Y^n) = S_{sn}(Y^n) \cup S_{dn}(Y^n) \cup S_d(Y^n) \cup S_l(Y^n) \cup S_u(Y^n).$$

先考察集合 $S_u(Y^n)$. 转换器防护范围的界限是从基本功能电路的输入端至转换器的输出端(不包括连至输出端的输出线), 这样, 根据输出所代表的实际意义, 当 Z 为非法输出时, E 不可能为合法输出. 而且电路必须保证, 当 Z 是危险合法输出时, E 不能为差错检测或定位指示输出. 因此, 可假设 $S_u(Y^n) = \Phi$.

再考察集合 $S_d(Y^n)$. 我们先给出若干假设和并发差错定位电路的有关概念.

假设 1 电路中的每一个故障均可按门级或开关级故障加以模型化.

假设 2 当一个影响转换器的故障发生后, 电路有足够的时间在基本功能电路或转换器产生另一个故障前, 使得转换器能够将其正常输入集中的所有输入加到它的输入端. 当一个影响基本功能电路的故障发生后, 电路有足够的时间在基本功能电路或转换器产生另一个故障前, 使得基本功能电路能够将其正常输入集中的所有输入加到它的输入端.

假设 3 对一个由多个物理模块组成的电路, 从某个模块产生第一个故障开始, 在一段时间内, 可能的后续故障仅产生于同一个模块中.

设基本电路的所有单故障所组成的故障集为 F, 产生内部故障后电路所实现的函数表示为 G_f. 并设 F_i 为物理模块 M_i ($i = 1, 2, \cdots, N$) 的单故障集. 那么, 基本电路的单故障集 $F = \cup_{i=1}^{N} F_i$.

通过对并发差错检测系统理论中的自测试和故障保险概念的修改, 可以形式化地定义原来属于定性描述的故障定位电路和完全故障定位电路概念.

定义 1 一个电路对应于 F 是故障定位的, 当且仅当 $\forall f \in F_i, i = 1, 2, \cdots, N, F = \cup_{i=1}^{N} F_i, \exists X \in S_n(X^m), G_f(X) \in S_{li}(Y^n)$.

定义 2 一个电路对 F 是完全故障保险的, 若对 $\forall f \in F_i, i = 1, 2, \cdots, N, F = \cup_{i=1}^{N} F_i, \forall X \in S_n(X^m)$, 有 $G_f(X) = G(X)$, 或者 $G_f(X) \in S_{li}(Y^n)$.

定义 3 一个电路对应于 F 是完全故障定位的, 当且仅当它对应于 F 是完全故障保险和故障定位的.

类似于并发差错检测系统理论中的部分自校验概念[3,6], 若缩小电路中所考虑的故障集的大小, 但不考虑单个模块中的多故障, 则可定义部分故障定位电路概念.

定义 4 一个电路是部分故障定位的, 当且仅当 $\forall f \in F_i^{\#}, F_i^{\#} \subseteq F_i, i = 1, 2, \cdots, N, F^{\#} = \cup_{i=1}^{N} F_i^{\#}, F = \cup_{i=1}^{N} F_i$, 1) 它对应于 $F^{\#}$ 是故障定位的, 且 2), $\forall f \in F_i^{*}, F_i^{*} \subseteq F_i^{\#}, i = 1, 2, \cdots, N, F^{*} = \cup_{i=1}^{N} F_i^{*}$, 它对应于 F^{*} 是完全故障保险的.

因此, 对理想的并发差错定位电路, 要求 $S_d(Y^n) = \Phi$. 这样, 对于一个基本健壮故障安全电路, 就有 $S(Y^n) = S_{sn}(Y^n) \cup S_{dn}(Y^n) \cup S_l(Y^n)$.

$S(W^w)$ 也是转换器的完全输入集, 它可划分为合法输入集 $S_n(W^w)$ 和非法输入集 $S_a(W^w)$ 两个互不相交的子集. 其中 $S_a(W^w)$ 可被划分为 M 个互不相交的子集, 即 $S(W^w) = \cup_{j=1}^{M} S_{aj}(W^w)$, 这些子集分别为基本功能电路的 M 个物理模块出错后功能电路的输出集.

$\forall X \in S(X^m)$, 有 $\Omega(X) = W$ 和 $\Theta_{sl}(W) = Y$, 或者 $G(X) = Y$. 如果 (Z, E) 被表示为 $(\Theta_{sl}^{Z}(W), \Theta_{sl}^{E}(W))$ 或 $(G^Z(X), G^E(X))$, 那么, 在正常情况下, 应有 $\Theta_{sl}^{Z}(W) = G^Z(X)$ 和 $\Theta_{sl}^{E}(W) = G^E(X)$.

3 健壮故障安全电路的基本特性

定义 5 一个电路对 F 是健壮故障安全的, 若对 $\forall f \in F_i, i = 1, 2, \cdots, N, F = \cup_{i=1}^{N} F_i, \forall X \in S_n(X^m)$, 有 $G_f(X) = G(X)$, 或者 $G_f(X) \in S_{sn}(Y^n) \cup S_{li}(Y^n)$.

定义 6 一个电路对应于 F 是完全健壮故障安全的, 当且仅当它对应于 F 是健壮故障安全和故障定位的.

上述定义表明, 在某个模块发生故障的情况下, 合法输入必将导致电路或者生成正确合法输出, 或者生成安全合法输出, 或者给出对应于该模块的差错定位子集中的输出, 且至少存在一个合法输入, 它能够使电路给出差错定位输出. 这意味着完全健壮故障安全电路中的所有故障是可定位的. 完全健壮故障安全电路将实现完全健壮故障安全目标, 该目标指的是在给定的故障假设下, 当完全健壮故障安全电路由于故障而产生第一个安全合法输出或者非法输出时, 该输出总是可以区分的, 即不同模块中的故障将导致电路产生属于不同的故障定位输出集中的输出.

若电路中存在冗余, 则它对故障集 F 是不具有故障定位特性的. 在假设 3 下, 可引入强健壮故障安全电路概念. 此类电路可实现完全健壮故障安全目标.

定义 7 一个电路由 N 个物理模块组成, 其故障集 $F = \cup_{i=1}^{N} F_i$. 它满足对一个故障序列 $\langle f_{i1}, f_{i2}, \cdots, f_{i(k-1)} \rangle, f_{ij} \in F_i, j = 1, 2, \cdots, k-1, 2 \leq k \leq \| F_i \|, i = 1, 2, \cdots, N, \forall X \in S_n(X^m)$, 有 $G_{\langle f_{i1}, f_{i2}, \cdots, f_{i(k-1)} \rangle}(X) = G(X)$, 或者 $G_{\langle f_{i1}, f_{i2}, \cdots, f_{i(k-1)} \rangle}(X) \in$

$S_{sn}(Y^n)$. 而对故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$, $\forall X \in S_n(X^m)$, 有 $G_{<f_{i1}, f_{i2}, \cdots, f_{ik}>}(X) = G(X)$, 或者 $G_{<f_{i1}, f_{i2}, \cdots, f_{ik}>}(X) \in S_{sn}(Y^n) \cup S_{li}(Y^n)$. 且 $\exists X \in S_n(X^m)$, 有 $G_{<f_{i1}, f_{i2}, \cdots, f_{ik}>}(X) \in S_{li}(Y^n)$. 则该电路对故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$ 是强健壮故障安全的.

定义 8　一个电路对 F 是强健壮故障安全的, 若它对由 F 中任意对应于某个物理模块的所有故障所组成的所有故障序列都是强健壮故障安全的.

如果限制电路中所考虑的某个模块的故障序列的长度, 或者缩小电路中所考虑的故障集, 但不考虑单个模块中的多故障, 那么, 可分别引入 k- 容错部分强健壮故障安全电路概念和部分健壮故障安全电路概念. 这两类电路可有限地实现完全健壮故障安全目标.

定义 9　一个电路由 N 个物理模块组成, 其故障集 $F = \cup_{i=1}^{N} F_i$. 设 k 是最小整数, 它满足对一个故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$, $f_{ij} \in F_i$, $j = 1, 2, \cdots, k$, $i = 1, 2, \cdots, N$. 实现函数 $G_{<f_{i1}, f_{i2}, \cdots, f_{ik}>}$ 的电路丧失强健壮故障安全特性, 且不存在一个输入矢量能定位该故障序列. 那么, 该电路是 k- 容错部分强健壮故障安全的, 如果该电路是健壮故障安全的, 且对任意模块 M_i 的任意故障序列和任何整数 q, $1 \le q \le k-1$, 或电路是健壮故障安全的, 或故障序列 $<f_{i1}, f_{i2}, \cdots, f_{iq}>$ 可被定位.

定义 10　一个电路是部分健壮故障安全的, 当且仅当 $\forall f \in F_i^{\#}$, $i = 1, 2, \cdots, N$, $F_i^{\#} \subseteq F_i$, $F^{\#} = \cup_{i=1}^{N} F_i^{\#}$, $F = \cup_{i=1}^{N} F_i$, (1) 它对应于 $F^{\#}$ 是故障定位的, 且 (2) $\forall f \in F_i^{*}$, $i = 1, 2, \cdots, N$, $F_i^{*} \subseteq F_i^{\#}$, $F^{*} = \cup_{i=1}^{N} F_i^{*}$, 它对应于 F^{*} 是健壮故障安全的.

若缩小电路中各个模块所考虑的故障集, 并考虑单个模块中的多故障, 则在这个精简的故障集 $F^{\#} \subseteq F$ 上, 我们还可定义精简强健壮故障安全电路和 k- 容错精简强健壮故障安全电路[5], 它们也可有限地实现完全健壮故障安全目标.

4　差错定位转换器的特性

转换器的主要功能是区分基本功能电路的输出矢量, 在确保基本电路不会产生不正确的合法输出的同时, 确定基本电路中的出错模块. 转换器的这一功能可用安全变量划分概念来表征. 可设转换器的单故障集为 $F\Theta_{sl}$.

定义 11　一个电路是安全变量划分的, 若它满足 (1) $\forall W \in S_n(W^w)$, 有 $\Theta_{sl}^{Z}(W) \in S_n(Z^u)$ 和 $\Theta_{sl}^{E}(W) \in S_n(E^v)$, 或者 (2) $\forall W \in S_{oj}(W^w)$, 有 $\Theta_{sl}^{Z}(W) \in S_{sn}(Z^u) \cup S_a(Z^u)$ 和 $\Theta_{sl}^{E}(W) \in S_{lj}(E^v)$, $j = 1, 2, \cdots, M$.

定义 12　一个电路是完全健壮故障安全的转换器, 若它是安全变量划分的、健壮故障安全的和故障定位的.

可以定义健壮故障安全转换器和故障定位转换器[5]. 如果转换器难以满足故障定位特性, 那么, 在满足假设 2 的前提下, 基本电路可采用具有强安全变量划分特性的转换器.

定义 13　一个电路由 $N-M(N>M)$ 个物理模块组成, 其故障集 $F\Theta_{sl} = \cup_{i=M+1}^{N} F_i$. 在无故障期间, 电路是安全变量划分的. 而对一个故障序列 $<f_{i1}, f_{i2}, \cdots, f_{i(k-1)}>$, $f_{ij} \in F_i$, $j = 1, 2, \cdots, k-1$, $2 \le k \le \| F_i \|$, $i = M+1, M+2, \cdots, N$, 它满足 $\forall W \in S_n(W^w)$, 有 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{i(k-1)}>}^{Z}(W) = \Theta_{sl}(W)$ 和 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{i(k-1)}>}^{E}(W) \in S_n(E^v)$; $\forall W \in S_{ar}(W^w)$, 有 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{i(k-1)}>}^{Z}(W) \in S_{sn}(Z^u) \cup S_a(Z^u)$ 和 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{i(k-1)}>}^{E}(W) \in S_{lr}(E^v)$, $r = 1, 2, \cdots, M$. 对故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$, 它满足 $\forall W \in S_n(W^w)$, 有 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}^{Z}(W) = \Theta_{sl}^{Z}(W)$ 和 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}^{E}(W) \in S_n(E^v) \cup S_{li}(E^v)$; $\forall W \in S_{ar}(W^w)$, 有 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}^{Z}(W) \in S_{sn}(Z^u) \cup S_a(Z^u)$ 和 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}^{E}(W) \in S_{lr}(E^v)$, 且 $\exists W \in S_n(W^w)$, 有 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}^{E}(W) \in S_{li}(E^v)$. 则电路对故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$ 是强安全变量划分的.

定义 14　一个转换器对 $F\Theta_{sl}$ 是强安全变量划分的, 若它对由 $F\Theta_{sl}$ 中任意对应于某个物理模块的所有故障所组成的所有故障序列都是强安全变量划分的.

定义 15　对故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ip}>$, 设 k 是一个最小整数, 它满足对一个故障序列 $<f_{i1}, f_{i2}, \cdots, f_{ik}>$, $f_{ij} \in F_i$, $i = M+1, M+2, \cdots, N$, $j = 1, 2, \cdots, k$, 实现函数 $\Theta_{sl<f_{i1}, f_{i2}, \cdots, f_{ik}>}$ 的转换器丧失安全变量划分特性, 且不存在一个输入矢量能定位该故障序列. 那么, 该转换器是 k- 容错部分强安全变量划分的, 如果该转换器是安全变量划分的, 且对任意故障序列和任何整数 q, $1 \le q \le k-1$, 或者转换器是安全变量划分的, 或者故障序列 $<f_{i1}, f_{i2}, \cdots, f_{iq}>$ 可被定位.

定义 16　一个电路是部分健壮故障安全转换器, 若它是安全变量划分的和部分健壮故障安全的.

类似地, 我们也可定义精简强安全变量划分转换器和 k- 容错精简强安全变量划分转换器[5].

5　基本功能电路与差错定位转换器互连的条件

文[5]给出并证明了如下定理.

定理 1　一个由完全(部分)健壮故障安全的基本功能电路和完全(部分)健壮故障安全的转换器所构成的基本电路是完全(部分)健壮故障安全的.

定理 2　一个由强健壮故障安全的基本功能电路和强安全变量划分的转换器构成的基本电路是强健壮故障安全的.

定理 3　一个由 k- 容错部分强健壮故障安全的基本功能电路和 k- 容错部分强安全变量划分的转换器所构成的基本电路是 k- 容错部分强健壮故障安全的.

定理 4　一个由精简强健壮故障安全的基本功能电路和精简强安全变量划分的转换器所构成的基本电路是精简强健壮故障安全的.

定理 5　一个由 k- 容错精简强健壮故障安全的基本功能电路和 k- 容错精简强安全变量划分的转换器所构成的基本电路是 k- 容错精简强健壮故障安全的.

6　应用实例分析

根据本文所提出的基本电路的模块结构, 电路的设计可分为基本功能电路的设计和转换器的设计两部分. 能够实现(含有限地实现)完全健壮故障安全目标的电路可分别由多种途径来实现. 以完全(部分)健壮故障安全电路设计为例. 文

[5]证明了完全(部分)故障定位电路是一类完全(部分)健壮故障安全电路.这样,一种可行的方案是用完全(部分)故障定位的功能电路与完全(部分)健壮故障安全的转换器互连来构造完全(部分) 健壮故障安全电路.

例 1 考虑如下基本电路:它满足 $M=1$ 和 $N=4$ 的划分,结构如图 1 所示.当 $M=1$ 时,不难证明,一个完全(部分)故障定位功能电路等价于一个完全(部分)自校验功能电路.因此,该电路的设计问题就进一步被简化为完全(部分)自校验的功能电路与完全(部分)健壮故障安全转换器的设计问题.

在图 1 中,BFC_1 和 BFC_2 是完全相同的两个无冗余电路,它们组成了基本功能电路,显然,该功能电路是完全自校验的.转换器由一个比较器和两个相同的校验器 $CHK1^*$ 和 $CHK2^*$(如图 3 所示)所组成.转换器的输入是功能电路的输出和时钟信号 F_e,输出有两个,一个是基本电路的功能输出 $(Z_1 \cdots Z_u)$,其中的各个分量是频率编码的,即用频率 F_e 信号表示危险输出(如 1 电平),用固定电平信号表示安全输出(如 0 电平);另一个是基本电路的差错定位指示输出 $(F_u^1, E_u^1, F_u^2, E_u^2)$,$v=8$.各个分量的值域为 $\{1^-, 0^-\}, 1^- \in \{(01),(10)\}, 0^- \in \{(00),(11)\}$.比较器采用文[9]所提出的强故障安全比较器(其位片结构如图 2 所示),$CHK1^*$ 和 $CHK2^*$ 采用文[2]所提出的具有内部故障指示的完全自校验校验器.$CHK2^*$ 的输入本身为双轨码,但 $CHK1^*$ 的输入端要加反相器才能把功能电路的双模冗余码输出转换为双轨码输出.在图 3 所示的校验器中,$u=2k+1\ (u\geq 5)$.$W(Q)$ 为它的编码输入,两个双轨码输出 F_u 和 E_u 分别用于指示内部差错和输入码字的合法性.与文[2]不同的是,图 3 中强自校验校验器所用的 u 个完全自校验校验器的结构如图 4 所示,其中,A 和 B 是普通的双轨码校验器,而 C 是一个特殊的双轨码校验器,它需附加一个交替变化的输入(本文直接选用 Fe 信号)[1,4,8].这就要求功能电路输出信号的持续有效期至少为一个 F_e 信号周期[4].

假定图 1 所示电路所考虑的故障集包括了除 F_e 信号输入线、转换器原始功能输出线、$CHK1^*$ 的输出线和 $CHK2^*$ 的输出线上的故障之外的所有单故障.那么,可以证明基本电路在 $M=1$ 和 $N=4$ 的划分条件下,图 1 所示的转换器是部分健壮故障安全的.据此,就可证明图 1 所示的基本电路也是部分健壮故障安全的[5].差错定位指示输出(故障症候)及其意义,它们所属的集合如表 1 所示.

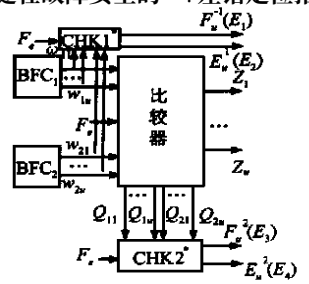

图 1 一个基本电路的组成与结构

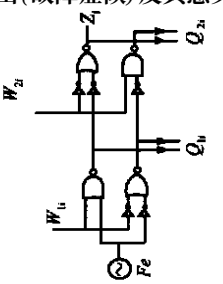

图 2 比较器的第 i 个位片结构

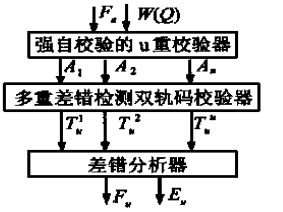

图 3 具有内部故障指示的完全自校验校验器

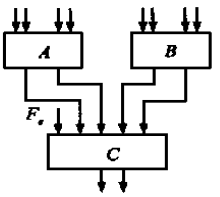

图 4 完全自校验校验器的结构

表 1 差错定位指示输出及其意义

F_u^1	E_u^1	F_u^2	E_u^2	意 义	$S_{li}(E^8)$
1^-	1^-	1^-	1^-	基本电路无差错	$S_{l0}(E^8)$
0^-	1^-	1^-	1^-	$CHK1^*$ 有故障	$S_{l1}(E^8)$
1^-	0^-	1^-	1^-	功能电路有故障,或 $CHK1^*$ 的 E_u^1 输出线有故障	$S_{l2}(E^8)$
1^-	1^-	0^-	1^-	$CHK2^*$ 有故障	$S_{l3}(E^8)$
1^-	1^-	1^-	0^-	比较器有故障,或 $CHK2^*$ 的 E_u^2 输出线有故障	$S_{l4}(E^8)$

从上述例子可以看出,广义故障安全系统理论不能直接用来说明上述基本电路的特性.因此,健壮故障安全系统理论具有更强的电路分析能力,以及更好的系统性和完整性.

7 结论

本文提出了一种健壮故障安全系统理论,该理论是广义故障安全系统理论的进一步发展.在现有的集成电路技术条件下,我们已获得了自校验电路和广义故障安全电路(如强故障安全电路)设计和实现的经验.本文研究所获得的结论和所给出的电路实例表明,我们可以用这些现存的、被验证过的电路来构造一些具有更加完善性能的电路.当然,有关健壮故障安全电路的系统的设计和实现方法是今后需要深入研究的课题.

作者简介:

江建慧 副教授,分别于 1985 年和 1988 年在上海铁道学院获得学士和硕士学位,于 1999 年在上海铁道大学获得博士学位.现任上海铁道大学计算技术研究所多值逻辑研究室主任.主要研究方向为容错计算、可信系统逻辑设计自动化.在国内学术刊物和国际学术会议上发表论文 30 多篇,协编出版有《计算机容错技术》专著一部.

施鸿宝 教授,博士生导师,现任上海铁道大学信息科学与技术学院副院长、计算技术研究所所长,上海市教育委员会重点学科《交通信息工程及控制》学术带头人.长期从事计算机软件与人工智能理论研究与应用工作.在国内外学术刊物发表论文 60 多篇,出版有《专家系统》、《神经网络及其应用》等专著三部. (下转第 42 页)

邮件发运方案代价的总和,代价越低,结果越好. 因 NN 法稳定性较差,十次实验结果均不相同,我们在 NN 法一栏使用了算术平均值,而 HA 稳定性较好,表中还同时给出了位置平均值(排序后中间次序的解)和此解出现的次数. 因第一组数据约束关系较简单,两种方法都得到了最优解;考查第二组、第三组数据,对于进一步处理后的领域解而言,神经网络方法解的质量比 HA 算法高,而第四组、第五组数据,神经网络方法难以准确满足约束条件,启发式算法总体效果要好些.

表 4 两种算法收敛速度比较

神经网络解法 NN		启发式算法 HA	
迭代次数	所占实验次数	迭代次数	所占实验次数
2000 以下	0	50 以下	20
2000～3000	10	50～100	30
3000～5000	29	100～200	0
5000 以上	11	200 以上	0

由表 4 可以看出,算法 HA 可以快速收敛,NN 方法软件模拟收敛较慢,实验中 NN 方法对参数较为敏感.

6 结论

本文首先对邮政运输调度问题进行了分析,给出了网状运输问题相应的数学模型,并由此构造出相应的神经网络模型. 针对问题的特点和此模型中存在的问题,提出一改进的启发式算法,实验结果表明启发式算法能快速收敛,稳定性好,易于得到合适解.

参考文献:

[1] Hopfield J J, Tank D W. Neural computation of decisions in optimization problems [M]. Biological Cybernetics, 1985, 52: 141 - 152.

[2] 程相君,王春宁,陈生谭. 神经网络原理及其应用[M]. 国防工业出版社, 1995.

[3] 陈国良. 神经计算机其在组合优化中的应用[J]. 计算机研究与发展, 1992(5): 1 - 21.

[4] Nirwan Ansari, Edwin S. H. Hou and Youyi Yu. A new method to optimize the satellite broadcasting schedules using the mean field annealing of a Hopfield neural network [J]. IEEE Trans. On Neural Networks, March 1995, 6(3): 470 - 482.

[5] 焦李成. 神经网络计算[M]. 西安电子科技大学出版社, 1993: 121 - 124.

作者简介:

陈 龙 1992 年毕业于华东师范大学计算机科学系,现任讲师. 主要研究方向为神经网络、遗传算法.

王国胤 1996 年毕业于西安交通大学,获工学博士学位. 现为重庆邮电学院副教授. 主要研究方向为神经网络、Rough Set、知识获取、智能信息系统.

刘心松 教授,博士生导师. 主要研究方向为三网合一、分布式计算机系统、神经网络.

聂 能 教授. 主要研究方向为智能信息系统.

(上接第 38 页)

参考文献:

[1] E. Fujiwara and K. Matsuoka. A self-checking generalized prediction checker and its use for built-in testing [J]. IEEE Transactions on Computers, 1987, 36(1): 86 - 93.

[2] N. Gaitanis. Totally self-checking checkers with separate internal fault indication [J]. IEEE Transactions on Computers, 1988, 37(10): 1206 - 1213.

[3] 胡谋. 计算机容错技术 [M]. 北京:中国铁道出版社, 1995.

[4] J. H. Jiang, M. Hu, and H. B. Shi. A novel structure of the hybrid logic networks based on the self-checking logic and fail-safe logic for fault diagnosis [A]. in Proceedings of the 5th International Conference on Computer-Aided Design and Computer Graphics [C], vol. 2, Beijing: International Academic Publishers, Shenzhen, Dec. 1997: 471 - 476.

[5] 江建慧. 并发差错控制理论及其多模冗余实现方法研究 [D]. 博士学位论文. 上海:上海铁道大学, 1999.

[6] P. K. Lala. Fault tolerant and fault testable hardware design [M]. NJ: Prentice-Hall, 1985.

[7] M. Lubaszewski and B. Courtois. A reliable fail-safe system [J]. IEEE Transactions on Computers, 1998, 47(2): 236 - 241.

[8] M. Nicolaidis. Fault secure property versus strongly code disjoint checkers [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 1994, 13(5): 651 - 658.

[9] M. Nicolaidis. Fail-safe interfaces for VLSI: Theoretical foundations and implementation [J]. IEEE Transactions on Computers, 1998, 47(1): 62 - 77.

[10] M. Nicolaidis, S. Noraz, and B. Courtois. A generalized theory of fail-safe systems [A]. in Proceedings of the 19th International Symposium on Fault Tolerant Computing, IEEE Computer Society Press, Chicago, June 1989, 398 - 406.