УДК 681.32.019.3

ОПЕРАТИВНЫЙ КОНТРОЛЬ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ИНФОРМАЦИОННОЙ ИЗБЫТОЧНОСТИ

Ю.П. БУЦЕНКО, Ю.Г. САВЧЕНКО

Рассмотрена задача обеспечения надежности компьютерных систем управления промышленного назначения. Предложено обобщение метода избыточных переменных на произвольные информационные процессы, независимо от способа их аппаратной или программной реализации.

Достоверность как один из показателей качества функционирования информационных и управляющих систем во многих случаях оказывается определяющим с точки зрения пригодности систем для использования в конкретных условиях. Если показатель надежности в значительной мере понимается во временном измерении, т.е. как способность объектом выполнять свои функции в течение заданного времени, то достоверность — это, прежде всего, вероятность отсутствия ошибки в определенном сообщении, управляющем воздействии, команде и т.п. К системам управления реальными объектами (промышленными, технологическими, оборонными, транспортными и т.п.) в отличие от информационных систем предъявляются исключительно высокие требования к их надежности, включая показатель достоверности. Речь идет, в первую очередь, о потенциально опасных производствах и процессах (энергетика, оборона, космос, продуктопроводы, государственные и интернациональные телекоммуникационные системы и т.д.), нарушение работоспособности которых приводит к угрозе жизни персонала, загрязнению окружающей среды или к значительным экономическим потерям. Среди главных причин нарушений можно выделить такие: физические (помехи промышленного и естественного происхождения, обрывы и короткие замыкания в каналах передачи информации, отказы и сбои оборудования); программные (остаточные ошибки в программах); человеческий фактор.

Все перечисленные причины проявляются, в конечном счете, как ошибки в результатах обработки информации, либо непосредственно в данных, поступающих, например, от технологических датчиков. Совершенно очевидно, что оперативное обнаружение таких ошибок является чрезвычайно важным с точки зрения безопасности системы в целом.

Для примера попытаемся определить, что важнее для относительно несложного прибора, называемого автопилотом самолета, его надежность

(среднее время безотказной работы, которое может составлять несколько сотен тысяч часов) или вероятность появления *необнаруженной* ошибки в управляющей команде. Без сомнения, ответ будет в пользу достоверности (безошибочности) информации, поступающей непосредственно на органы управления. Подчеркнем, что в случаях, когда речь идет о безопасности, ошибка должна быть обнаружена сразу же *в момент ее возникновения*, чтобы не допустить ее воздействия на органы управления путем блокировки и перехода, например, на ручное управление. Это чрезвычайно важный момент — именно *оперативность* обнаружения или контроля определяет, в конечном счете, безопасность того или иного технического объекта. «Контроль призван защитить нас от аварий в тех случаях, когда из-за недостаточной надежности в изделии появляются отказы» [1] — эта мысль определяет актуальность рассматриваемого ниже подхода.

Сегодня для каждой из перечисленных выше причин нарушений работоспособности разработан, на первый взгляд, достаточно обширный арсенал методов их нейтрализации. Но это не совсем так. Например, для борьбы с физическими причинами применяются методы введения структурной избыточности, помехозащищенное кодирование, реконфигурация телекоммуникационных сетей и т.п. Но далеко не все эти методы учитывают специфику именно компьютерных систем. Например, классический метод «горячего» резервирования не так просто применить, если резервируется такой компонент структуры, как компьютер. В этом случае резервный компьютер действительно должен быть «горячим» (способным с минимальной задержкой во времени выполнять функции отказавшего основного компьютера), а для этого необходимо обеспечить полную тождественность данных, которые сохраняются в памяти основного и резервного компьютеров, т.е. они должны функционировать параллельно. Для того, чтобы определить правильно работающий компьютер, необходим еще и арбитр, который это определит. Но и он может отказать. Поэтому в таких случаях используются преимущественно структурные методы обеспечения надежности (резервировании на аппаратном уровне) [2]. Например, в системе автоматического управления полетом (автопилотом) самолета Boueng 737/300 стандартный блок содержит два канала вычислений, реализованных тремя центральными процессорами. Один из них обеспечивает всю систему программного управления полетом, остальные — только критические функции. Этот стандартный блок резервирован, нейтрализация ошибок выполняется мониторами, которые сравнивают сигналы, а в каждом стандартном блоке два таких монитора [3].

В этом, как и во всех аналогичных случаях, целью введения структурной избыточности является сохранение возможности системой выполнять заданные функции при возникновении ошибок как результата неисправностей. Ошибки в данном случае обнаруживаются и, по сути, исправляются (нейтрализуются), а постоянные неисправности устраняются в процессе последующего технического обслуживания.

Для защиты информации от ошибок при ее сохранении сегодня достаточно широко используются системы с архитектурой RAID (redundant array of inexpensive disks — матрица недорогих дисков с избыточностью), что не

только защищает информацию от ошибок в результате случайных сбоев, но и дает важную информацию о состоянии жестких дисков [4].

Примеры использования структурной избыточности в современных информационных и управляющих системах можно продолжать достаточно долго. Отметим общее, что характерно для этого класса методов. Главной целью остается нейтрализация ошибок и сохранение работоспособности при отказе некоторой части оборудования, а не оперативность обнаружения ошибок. Для достижения данной цели приходится платить большую цену — высокий уровень избыточности (аппаратурные затраты, как правило, превышают трехкратные).

В то же время существует весьма обширный класс задач, где сохранение работоспособности при отказе части оборудования системы не является остро необходимым — достаточно своевременно обнаружить ошибку и заблокировать ее воздействие на объект управления. В этом случае могут быть получены достаточно экономные технические реализации соответствующих процедур контроля. Как показано ниже, такие процедуры могут быть построены на основе использования информационной избыточности.

Понятие информационной избыточности (ИИ) базируется на уменьшении реальной энтропии сообщений по сравнению с максимальной энтропией, когда все возможные сообщения равновероятны. В соответствии с работой [5] численно значение ИИ можно определить из простого соотношения

$$D = 1 - \frac{H_r}{H_{\max}},$$

где $H_r = -\sum_{i=1}^{N} p_i \log_2 p_i$, $H_{\max} = \log_2 N$, p_i, $i = \overline{1, N}$ — вероятность появления i-го сообщения; N — количество всех возможных сообщений, генерируемых источником.

Уже сам по себе факт наличия ИИ позволяет в определенной мере контролировать достоверность поступающих сообщений. Действительно, любые отклонения вероятностного распределения от равномерного могут свидетельствовать об ошибках. Однако этот критерий с практической точки зрения не имеет перспективы, поскольку требует длительного наблюдения за поступающими сообщениями, что исключает оперативное обнаружение ошибки в момент ее возникновения. Кроме того, одиночные ошибки не будут обнаруживаться, поскольку их влияние на статистическое распределение ничтожно мало.

Отметим важный момент: если в результате ошибки появляется сообщение, вероятность появления которого в нормальных условиях равна нулю, то ситуация меняется кардинально — ошибка может быть обнаружена сразу же, т.е. в момент ее возникновения. В терминах теории кодов с коррекцией ошибок такое сообщение является запрещенным словом. Для случая передачи информации по каналам связи задача оперативного обнаружения ошибок решается традиционными методами помехозащищенного кодирования. Если объектом контроля является преобразователь информации (цифровое устройство, компьютер, система управления или регулиро-

вания), оперативный контроль достоверности существенно усложняется. И если для контроля сравнительно простых цифровых схем может быть использован также кодовый подход [6], то для компьютерных систем управления универсальных подходов пока не существует. Покажем, что попытка найти такой подход может быть предпринята на базе обобщения понятия ИИ на вычислительные процедуры и алгоритмы независимо от способа их реализации (аппаратной или программной).

Предлагаемая идея оперативного контроля развивает достаточно «старый» (и на данный момент «хорошо забытый») метод избыточных переменных, который в свое время был использован для контроля правильности решений систем дифференциальных уравнений [7]. В кратком изложении этот метод сводится к следующему.

При решении системы из *n* уравнений (не обязательно дифференциальных) добавляется еще одна переменная и еще одно уравнение, искусственно связывающее добавленную переменную с исходными переменными. Теперь, получив результат решения системы, достаточно проверить его на выполнение введенного соотношения, чтобы убедиться в достоверности результата. Для иллюстрации приведем простейшие примеры.

1. Пусть требуется вычислить (программно или аппаратно) значения двух величин, исходя из таких соотношений

$$z_1 = x^2{}_1 + x^2{}_2, \quad z_2 = 2x_1x_2 .$$

Добавим к ним еще одно «избыточное» соотношение

$$z_3 = z_1 + z_2 = x^2{}_1 + 2x_1x_2 + x_2{}^2 = (x_1 + x_2)^2.$$

Тогда, вычислив все три величины, правильность результата можно проверить с помощью простого контрольного соотношения $r = z_3 - z_1 - z_2$.

Если ошибок нет (точнее, не обнаружено), то $r = 0$, и если ошибка обнаружена, то $r \neq 0$,

Отметим, что при $r = 0$ полной уверенности в отсутствии ошибок не может быть, поскольку с некоторой вероятностью возможны ошибки, которые не изменяют контрольное соотношение.

2. Требуется вычислить значения двух экспонент

$$y_1 = e^{x_1} \text{ и } y_2 = e^{x_2} .$$

Добавим еще одну искусственную переменную

$$y_3 = y_1y_2 = e^{x_1+x_2} .$$

Тогда после вычисления всех трех величин достаточно проверить выполнение соотношения

$$y_3 - y_1y_2 = 0,$$

чтобы проверить правильность проведенных вычислений.

3. Вычисляются (аппаратно или программно) значения булевых переменных

$$y_1 = x_1(\bar{x}_2 \vee x_3), \quad y_2 = \bar{x}_1x_2 \vee \bar{x}_2x_3, \quad y_3 = \bar{x}_1\bar{x}_2 \vee x_2x_3 .$$

Как и в предыдущих примерах добавим еще одну булеву переменную y_4, «связывающую» y_1, y_2, y_3

$$y_4 = y_1 \oplus y_2 \oplus y_3.$$

После подстановки соответствующих выражений для y_1, y_2, y_3 и упрощений получим

$$y_4 = \bar{x}_2 \vee x_1 x_3.$$

Тогда

$$r = y_1 \oplus y_2 \oplus y_3 \oplus y_4.$$

Как и в предыдущих примерах, $r \neq 0$ будет свидетельствовать о наличии ошибки в вычислениях.

Приведенные примеры заведомо упрощены и носят чисто иллюстративный характер, демонстрируя лишь саму идею введения избыточных переменных. Общий и более глубокий смысл этой идеи состоит в создании условий, искусственно ограничивающих диапазон возможных значений результатов проводимых вычислений. Введенные ограничения в дальнейшем выступают в качестве контрольных соотношений для проверки правильности проведенных процедур.

Для обобщения достаточно очевидной идеи рассмотрим некоторое произвольное преобразование совокупности (вектора) входных данных (переменных) $X = \{X_1, X_2, ..., X_l\}$ в совокупность (вектор) результата $Y = \{Y_1, Y_2, ..., Y_k\}$

$$Y = F(X). \qquad (1)$$

Очевидно, некоторый абстрактный «пользователь», для которого выполняются преобразования, не зная входных данных (сигналов), не может судить о правильности результата вычислений. А если данные известны, то для контроля ему необходимо самостоятельно провести вычисления результата, т.е. повторить процедуру (1). В данном случае требуется такое же время либо такая же аппаратура (по сложности) для получения независимого результата. В ряде случаев это либо недопустимо по времени (теряется оперативность), либо по аппаратным затратам, что определяет целесообразность (а в некоторых случаях и необходимость) использования идеи избыточных переменных.

Рассмотрим произвольное преобразование входных данных (сигналов), представленное некоторой системой уравнений (1) общего вида, включая случай, когда каждая компонента результата вычисляется независимо от других. Однако общими остаются значения входных переменных (сигналов) — это принципиально важное требование.

К этим уравнениям добавляется некоторое количество избыточных уравнений и, соответственно, переменных. Избыточные уравнения «связывают» исходные функции некоторой композиционной функцией (КФ), например, суммой или произведением. Одним из основных критериев при выборе РФ, очевидно, должна быть сложность реализации выбранной композиции. Ориентиром здесь может служить повторная реализация ис-

ходных функций с последующим их объединением операцией композиции (суммой, произведением и т.п.). Такой прямолинейный путь имеет, по крайней мере, два недостатка.

Во-первых, большая сложность реализации (такое же время, как и при реализации исходного преобразования, или удвоение оборудования). Во-вторых, и это главное, вероятность возникновения точно такой же ошибки при повторных вычислениях может оказаться достаточно большой, если ошибка имеет одну и ту же первопричину (например, неисправность внешних по отношению к исходному преобразователю информации блоков или сбои при выполнении внешних по отношению к программам, реализующих (1) процедурам). С этой точки зрения, вычисления исходных функций в составе КФ желательно провести «другим способом» для того, чтобы минимизировать вероятность возникновения однотипных ошибок. Т.е. в результате композиции должна образоваться некоторая новая функция, которая *проще* суммы функций, объединяемых композицией.

В общем случае (для произвольных преобразований) вряд ли можно дать рецепт выбора КФ. Однако для частных случаев, интересных с точки зрения практического применения, можно попытаться сформулировать некоторые ориентиры для такого выбора.

Если все функции, описывающие преобразование (1), являются аналитическими и такими, которые допускают аппроксимацию степенным рядом Тейлора, т.е. некоторой суммой переменных в различной степени, то в качестве композиции также целесообразно использовать сумму выходных переменных. То же можно рекомендовать и в случаях цифровой обработки сигналов, когда в качестве стандартного используется представление в частотной области в виде преобразования Фурье и БПФ. В других случаях, по-видимому, следует искать другие КФ.

Если же исходное преобразование задано булевыми функциями, то этот случай исследован достаточно подробно. Заметим, что для булевых функций чаще всего используют в качестве КФ сумму по модулю 2 или произвольные логические функции при применении нелинейных кодов [6, 8].

Однако, несмотря на достаточно большое многообразие классов возможных исходных функций, которые должна «связать» КФ, можно сформулировать некоторые общие требования к выбору КФ.

1. КФ должна зависеть от отклонений всех вычисляемых переменных от их истинных (правильно вычисленных) значений. Такое требование естественно назвать *девиационной тотальностью*.

2. В частности, КФ должна охватывать все переменные (*вариационная тотальность*). На первый взгляд, это требование не является обязательным. Однако на практике, именно оно может оказаться важным с точки зрения безопасности. В том же примере с автопилотом совокупность контролируемых управляющих воздействий зависит от многих факторов (высоты, скорости, метеоусловий и т.п.) и вряд ли на каких-либо участках полета допустима ошибка в части управляющих команд.

3. КФ должна присутствовать (возможно, неявным образом) во всех соотношениях системы. Такое требование (его можно назвать *системной тотальностью*) гарантирует влияние всех выполняемых при вычислениях процедур на результат контроля. А это, в свою очередь, непосредственно связано с его полнотой.

4. При выборе КФ необходимо обеспечить невозможность взаимной компенсации ошибок. С этой точки зрения, например, естественным является применение такого контрольного показателя, как сумма квадратов невязок (разностей между левой и правой частями) для всех уравнений системы. Это свойство может быть названо *обоснованностью* КФ.

Перечисленные свойства желательно дополнить требованием *дискреционности* — возможностью определять переменную, для которой имеет место отклонение от истинного значения, если такое отклонение (ошибка) является существенным для безопасности.

Важным моментом при выборе числа избыточных переменных и соответствующих КФ является также достигаемая полнота контроля, т.е оценка части обнаруживаемых ошибок по отношению ко всем возможным. По сути, это и есть тот положительный эффект в чистом виде, ради которого вводятся избыточные переменные. Временные или аппаратные затраты на их введение — цена, которую необходимо заплатить за полученный эффект. С этой точки зрения может быть сформулирована задача оптимизации: найти такую КФ, которая бы обеспечивала заданную полноту контроля при минимальных затратах (временных или аппаратных). Однако полнота контроля как процент обнаруживаемых ошибок во многих случаях оказывается слишком грубым показателем для оценки реальной эффективности контроля, учитывая различную опасность конкретных ошибок для конечного пользователя.

Можно ожидать, что все приведенные соображения и требования к выбору КФ в совокупности могут привести к достаточно сложной ее структуре, и что наиболее адекватным подходом окажется рандомизация с последующим применением аппарата нечеткой логики.

В завершение, как пример «хорошего» (оптимального) выбора КФ можно упомянуть идею организации контроля вычислений при решении задач из области энергетики, содержащуюся в одной из ранних работ П. Элайса [9]. Эта практически очевидная идея состоит в использовании в качестве контрольного соотношения (по сути, КФ) закона сохранения энергии, невыполнение которого однозначно свидетельствует об ошибке вычислений. Интересным здесь является тот факт, что в этом случае нет необходимости вводить искусственные избыточные переменные.

ЛИТЕРАТУРА

1. *Крохин Я.А.* Фактометрия. Техногенные катастрофы. Между прошлым и будущим. — Киев: Логос, 2004. — 92 с.
2. *Shooman M.L.* Reliability of Computer Systems and Networks: Fault Tolerance, Analysis and Design. — John Wiley & Sons. INC, 2002. — 528 p.

3. *Авиженис А.* Гарантоспособные вычисления: От идей до реализации в проектах. В кн. Отказоустойчивость в СБИС / Пер. с англ. — М.: Мир, 1986. — С. 8–21.
4. *Chen P.M., Lee E.K., Gibson G.A., Katz R.H., Patterson D.A*. RAID: High-Performance, Reliable Secondary Storage ACM Computing Surveys, 26(2): 1994. — P. 145–185.
5. *Шеннон К.* Математическая теория связи. В кн. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 243–332.
6. *Савченко Ю.Г.* Цифровые устройства, нечувствительные к неисправностям элементов. — М.: Сов. Радио, 1977. — 170 с.
7. *Бритов Г.С. и др*. Метод избыточных переменных и его сравнение с методами кодирования. Доклад на IV-ом симпозиуме по использованию избыточности в информационных системах. — Л.: ЛИАП, 1968. — С. 79–87.
8. *Локазюк В.М., Савченко Ю.Г.* Надійність, контроль, діагностика і модернізація ПК. — Київ: Видавничий центр «Академія», 2004. — 375 с.
9. *Элайс П.* Кодирование в реальних системах святи. В кн. Кибернетический сборник, № 4. — М.: ИЛ, 1962. — С. 7–32.

Поступила 17.12.2009