УДК 621.396

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ МЕТОДА СИНГУЛЯРНЫХ РАЗЛОЖЕНИЙ ПРИ ОПРЕДЕЛЕНИИ ПАРАМЕТРОВ МОДЕЛИ УСТРОЙСТВА ЗАЩИТЫ

В.С. Бреславец
(представил д.т.н., проф. В.А. Кравец)

Предлагается использование метода сингулярных разложений (SVD) при определении передаточной функции информационного канала связи с элементами защиты.

Разработка математического и программного обеспечения для автоматизации решения задач защиты информационных каналов связи это необходимый этап развития методов анализа влияния нелинейных характеристик элементов защиты на качество передаваемой информации. При этом построение передаточной функции для учета влияния нелинейных характеристик устройств защиты приводит к необходимости аппроксимации ее линейной комбинацией **n** заданных базисных функций φ_i, которые в общем случае могут быть нелинейными функциями от **t**

$$y_i \approx c_1\varphi_1(t)+c_2\varphi_2(t)+\ldots+c_n\varphi_n(t). \qquad (1)$$

Для определения коэффициентов аппроксимации c_j наиболее часто используется метод наименьших квадратов.

Имеется много различных алгоритмов для вычисления набора коэффициентов, дающего минимальную сумму квадратов. При этом наиболее перспективным является применение математического анализа. Пусть

$$r=\left(\sum_{i=1}^{m}\left(\sum_{j=1}^{n}c_j\varphi_j(t_i)-y_i\right)^2\right)^{1/2}. \qquad (2)$$

Минимизируя **r** (или, что все равно минимизируя r^2) потребуем, чтобы для **k = 1, …, n**

$$\partial r^2/\partial c_k = 0.$$

Беря производные и изменяя порядок суммирования, получаем

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m}\varphi_j(t_i)\varphi_k(t_i)\right)c_j=\sum_{i=1}^{m}y_i\varphi_k(t_i). \qquad (3)$$

Эту систему из **n** линейных уравнений с **n** неизвестными c_j можно записать в матричной форме

$$\mathbf{Pc=q}, \qquad (4)$$

где

$$p_{kj} = \sum_{i=1}^{m} \varphi_k(t_i)\varphi_j(t_i); \qquad (5)$$

$$q_k = \sum_{i=1}^{m} \varphi_k(t_i) y_i . \qquad (6)$$

Уравнения **Pc = q** называются нормальными уравнениями, причем матрица **P** зависит лишь от базисных функций, так как значения y_i в неё не входят. Наиболее надежный метод для вычисления коэффициентов в общей задаче наименьших квадратов основан на матричной факторизации, называемой сингулярным разложением.

Метод сингулярного разложения или SVD (Singular Value Decomposition) начинается с разложения матрицы, известной в статистическом анализе экспериментов как матрица плана. Это прямоугольная матрица из m строк и n столбцов, элементы которой суть

$$a_{ij} = \varphi_j(t_i). \qquad (7)$$

Если через **y** обозначить вектор размерности **m** с элементами y_i, а через **c** – вектор размерности **n** с компонентами c_j, то приближенные равенства

$$\sum_{j=1}^{n} c_j \varphi_j(t_i) \approx y_i, \qquad i = \overline{1, m}, \qquad (8)$$

можно переписать в виде

$$\mathbf{Ac} \approx \mathbf{y} . \qquad (9)$$

Подпрограмма SVD, исходя из входной матрицы **A**, получает на выходе три матрицы **S**, **U**, **V**. Матрица **S** – диагональная с неотрицательными диагональными элементами, называемыми сингулярными числами матрицы **A**. Матрицы **U**, **V** используются для преобразования уравнений $\mathbf{Ac} \approx \mathbf{y}$ в эквивалентную диагональную систему

$$\sum \bar{c} \approx \bar{y} . \qquad (10)$$

Пусть s_j, $j = 1, \ldots, n$, - диагональные элементы **S**. При этом, если все s_j отличны от нуля, то можно разрешить преобразованные уравнения, полагая

$$\bar{c}_j = \bar{y}_j / \sigma_j, \qquad j = \overline{1, n} . \qquad (11)$$

Однако, это не всегда желательно, если некоторые σ_j малы. При этом все σ_j не равны нулю тогда и только тогда, когда базисные функции φ_j линейно независимы в заданных точках.

Множество векторов будет линейно независимыми, если ни один из них не может быть представлен в виде линейной комбинации других.

Предполагаем два вектора не зависимыми, если они перпендикулярны или ортогональны. Используем индекс **T**, чтобы обозначать транспо-

нирование вектора или матрицы. Два вектора **u** и **v** будут ортогональными, если их скалярное произведение равно нулю, т.е. если

$$\mathbf{u}^T \mathbf{v} = \mathbf{0}. \quad (12)$$

Далее, вектор **u** имеет длину 1, если $\mathbf{u}^T\mathbf{u} = \mathbf{1}$. Квадратная матрица будет ортогональной, если ее столбцы суть попарно ортогональные векторы длины 1. Таким образом, матрица **U** ортогональна, если

$$\mathbf{u}^T\mathbf{u} = \mathbf{I}, \quad (13)$$

где **I** – единичная матрица. Заметим, что ортогональная матрица автоматически не вырождена, поскольку $\mathbf{U}^{-1} = \mathbf{U}^T$.

Умножение на ортогональные матрицы не изменяет такие важные геометрические величины, как длина вектора или угол между двумя векторами. При этом ортогональные матрицы не увеличивают величины ошибок [1].

Для любой матрицы A и любых двух ортогональных матриц **U** и **V** рассмотрим матрицу **Σ**, определяемую соотношением

$$\mathbf{\Sigma} = \mathbf{U}^T\mathbf{A}\mathbf{V}. \quad (14)$$

Если $\mathbf{u}_j$ и $\mathbf{v}_j$ суть столбцы матриц **U** и **V** соответственно, то отдельные компоненты матрицы **S** равны

$$\sigma_{ij} = \mathbf{u}_i^T \mathbf{A}\mathbf{v}_j. \quad (15)$$

При этом надлежащим выбором матриц **U** и **V** можно обратить большинство элементов σ_{ij} в нули, а также можно даже сделать **Σ** диагональной с неотрицательными диагональными элементами.

Сингулярным разложением действительной **m × n** - матрицы **A** будет всякая ее факторизация вида

$$\mathbf{A} = \mathbf{U}\,\mathbf{\Sigma}\mathbf{V}^T, \quad (16)$$

где **U** - ортогональная **m × m** - матрица, **V** - ортогональная **n × n** - матрица, а **Σ** —диагональная **m × n** - матрица, у которой $\sigma_{ij} = \mathbf{0}$ при $\mathbf{i} \neq \mathbf{j}$ и $\sigma_{ii} = \sigma_i \geq \mathbf{0}$. Величины σ_i являются сингулярными числами матрицы **A**, а столбцы матриц U и **V** - левыми и правыми сингулярными векторами.

Пусть **A** - заданная **m × n** матрица, причем **m ≥ n**, а **b** – заданный вектор размерности **m**. Нужно найти все векторы **x**, для которых

$$\mathbf{A}\mathbf{x} = \mathbf{b}. \quad (17)$$

Система уравнений **Σz = d**, где **z = VTx** и **d = UTb** диагональная и, следовательно, легко решается [2].

Поскольку в основном уравнении, вводящем сингулярное разложение, матрица **V** снабжена индексом **T**, то в уравнение входят столбцы обеих матриц **U** и **V**, а не строки одной и столбцы другой. Ядро матрицы **A** есть множество векторов **x**, для которых **Ax** = 0, а область значений **A** - это множество векторов **b**, для которых система **Ax = b** имеет решение.

Входом в SVD являются **m** × **n** матрица A, информация о размерностях и две логические переменные, указывающие, нужно ли вычислять

матрицы **U** и **V**. Выходом будут сингулярные числа (обычно, хотя и не обязательно, в убывающем порядке), **m** × **n**-матрица **U** и **n** × **n** - матрица **V**. В случае большой задачи любую из матриц **U** и **V** можно формировать на месте матрицы **A**. Процедуру легко можно модифицировать таким образом, чтобы получить полную **m** × **m** - матрицу **U**.

Выходной информацией является информация, выводимая на экран в виде сообщений и окон с результатами вычислений в ходе диалога с пользователем. Также выходной информацией являются текстовые файлы транслированной процедурой на нужный язык программирования.

Программная часть данной работы реализована в программном файле svd.pas состоящем из: иллюстрирующей программы для процедуры SVD; программную оболочку; саму процедуру SVD.

Процедура SVD состоит из ряда блоков.

Один из сегментов программы находит наибольшее сингулярное число, которое будет участвовать в выявлении пренебрежимо малых сингулярных чисел. Здесь также присваивается нулевое значение вектору коэффициентов, что будет конечным результатом, если все сингулярные числа окажутся пренебрежимо малыми. Другой сегмент применяет к исходным данным преобразование **U**, находит преобразованные коэффициенты, а затем применяет преобразование V, чтобы получить сами коэффициенты. Следующий фрагмент находит пренебрежимо малые сингулярные числа. Для каждого найденного печатается список коэффициентов, называемых нулевыми. Любое кратное (**a**) этих коэффициентов можно добавить к напечатанным прежде, не увеличивая **r** более чем на **aT**. Коэффициенты нормируются так, что сумма их квадратов равна 1.0.

Входом в процедуру SVD являются **m** × **n** матрица **A**, информация о размерностях и две логические переменные, указывающие, нужно ли вычислять матрицы **U** и **V**. На выходе процедуры - сингулярные числа **m**, **n** - матрицы **U** и **n** × **n** - матрицы **V**. В случае большой задачи любая из матриц **U** и **V** формируется на месте матрицы **A**, а процедура модифицируется таким образом, чтобы получить полную **m** × **m** - матрицу **U**.

Таким образом, разработанное программное обеспечение позволяет автоматизировать процесс определения параметров модели.

ЛИТЕРАТУРА

1. Ошибки округления в алгебраических процессах // Сб. докладов под ред. В.В. Воеводина. – 1968. – М.: ВЦ МГУ – С. 39 - 58.

2. Уилкинсон Дж. Алгебраическая проблема собственных значений. Пер. с англ. – М.: Наука, 1970. – 264 с.

Поступила в редколлегию 4.6.2000