Speeding up elliptic cryptosystems by using a signed binary window method, Advances in Cryptology. – CRYPTO'92, LNCS 740. – 1993. – P. 345–357. 6. Кнут Д. Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы. – М.: Мир, 1976. 7. Juan Manuel Garcia Garcia, Rolando Mechaca Garcia Parallel Algorithm for Multiplication on Elliptic Curves. 8. Nelasa A.V., Dolgov V.I. Multisequencing of operation of a scalar multiplication on elliptic curve//Proceedings of the International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics" (CADSM'2005). – Lviv-Polyana, 2005. – P. 122–123. 9. Библиотека многократной арифметики MMATH v. 1.12 (12 августа 1996 г.) © АО "ИИТ" (г. Харьков) 10. Пинчук В.П. Библиотека VP / C++. Модуль syst.h. – Запорожье: ЗНТУ, 2003.

УДК 519.8766.5

М.П. Дивак, Ю.П. Франко, М.Я. Шпінталь

Тернопільська академія народного господарства

ОЦІНЮВАННЯ ДОПУСТИМИХ ЗНАЧЕНЬ ПАРАМЕТРІВ БАГАТОЕЛЕМЕНТНОЇ СТАТИЧНОЇ СИСТЕМИ НА ОСНОВІ АНАЛІЗУ ЇЇ ІНТЕРВАЛЬНИХ ХАРАКТЕРИСТИК

Розглянуто задачу допустимого оцінювання параметрів статичної багатоелементної системи. Запропоновано метод допустимого оцінювання параметрів складних систем, в якому допустимі області оцінок параметрів подані у вигляді багатовимірних еліпсоїдів.

The task of tolerance parameters estimation of the static multi-element systems based on the interval analysis is considered. Method of tolerance estimation of the parameters of the complex systems is proposed. In the method the tolerance estimation sets in form of multidimensional ellipsoids is represented.

Постановка проблеми

Однією із проблем синтезу складних багатоелементних статичних систем є проблема знаходження таких значень її параметрів, які забезпечать задані характеристики – виходи усієї системи [1]. Надалі під параметрами системи розумітимемо характеристики її складових елементів, підсистем, модулів. Враховуючи, що під час виготовлення елементів системи виникають випадкові технологічні відхилення їх характеристик від розрахункових, то природним є ризик, що побудована система може бути функціонально непридатною. Як відомо, достатньо часто функціональна придатність системи задається імовірністю її працездатності [2]. За цих умов синтез складних статичних систем полягає у знаходженні допустимих значень параметрів підсистеми, які забезпечуватимуть допустимі характеристики системи із заданою імовірністю її працездатності [1].

Для синтезу допустимих значень параметрів системи використовують гарантований та стохастичний підходи [2]. Перший полягає у знаходженні таких допустимих значень параметрів системи, які забезпечують повну гарантію працездатності. Однак при цьому отримуватимемо надзвичайно жорсткі вимоги до технологічного процесу синтезу елементів системи. У разі стохастичного підходу традиційні методи вимагають надзвичайно складних процедур розв'язування задач нелінійного програмування високої розмірності. Враховуючи, що значення виходів системи є встановленими в певних межах допустимих значень, тобто у вигляді числових інтервалів, для вирішення вказаної проблеми можливим є застосування методів аналізу інтервальних даних [2].

Під час розв'язування задач синтезу допустимих значень параметрів елементів математичні моделі статичних систем зображають системами інтервальних рівнянь [2]. Для оцінювання розв'язків інтервальних систем можливим є застосовування відомих методів допустимого оцінювання.

Враховуючи недоліки існуючих інтервальних методів допустимого оцінювання, огляд яких повною мірою наведено у [1; 2], актуальним є розвиток еліпсоїдних методів. Останні є придатнішими в задачах синтезу допусків, особливо у разі сильної "витягнутості" множини розв'язків інтервальної системи, оскільки забезпечують значно більше покриття допустимої області, ніж традиційні методи, побудовані на "вписуванні" у допустиму область прямокутних паралелепіпедів ("брусів") з гранями, паралельними до осей координат [3].

Постановка задачі

Розглянемо статичну систему, яка описується нелінійними залежностями $g_i(\vec{b})$ її вихідних характеристик y_i (виходів) від характеристик $\vec{b}=(b_1,..,b_m)^T$ елементів чи підсистем, які вважатимемо параметрами системи [1]

$$y_i = g_i(\vec{b}),\ \ i=1,...,N\ .$$

Нехай для побудови системи спочатку проводиться синтез її окремих елементів. Для заданих номінальних значень виходів $y_{0i}=g_i(\vec{b}_0)$ розраховують номінальні значення параметрів $\vec{b}_0=(b_{01},..,b_{0m})^T$ системи. У процесі виготовлення елементів системи виникають випадкові технологічні відхилення $\delta\vec{b}$ від номінальних $\vec{b}_0$ значень. Припустимо, що ці відхилення відповідають нормальному закону. В цих умовах задають допустимі з точки зору функціональної придатності об'єкта інтервали виходів $y_{0i}\in[\,y_i^-,y_i^+\,]$ і визначають множину допустимих значень вектора параметрів із розв'язку такої інтервальної системи [2]:

$$y_i^- \le g_i(\vec{b}) \le y_i^+,\ \ i=1,...,N\ .$$

Застосуванням розкладу функцій $g_i(\vec{b})$ в ряд Тейлора в околі вектора номінальних значень параметрів $\vec{b}_0$ та з вибором першого члена розкладу приходимо до такої системи

$$y_i^- \le y_{i0} + \sum_{j=1}^{m} \left.\frac{\partial g_i(\vec{b})}{\partial b_j}\right|_{\vec{b}=\vec{b}_{0j}} (b_j - b_{0j}) \le y_i^+,\ i=1,...,N\ .$$

Введемо позначення

$$\delta y_i^- = y_i^- - y_{i0},\ \delta y_i^+ = y_i^+ - y_{i0},\ \delta b_j = b_j - b_{0j},\ \phi_{ij} = \left.\frac{\partial g_i(\vec{b})}{\partial b_j}\right|_{\vec{b}=\vec{b}_{0j}},\ i=1,...,N$$

і перепишемо лінеаризовану систему нерівностей у матричному вигляді

$$\delta\vec{Y}^- \le \tilde{F}\cdot\delta\vec{b} \le \delta\vec{Y}^+\ , \qquad (1)$$

де $\delta\vec{Y}^- = \{\delta y_i^-, i=1,\ldots,N\}, \delta\vec{Y}^+ = \{\delta y_i^+, i=1,\ldots,N\}$ – вектори, складені із верхніх та нижніх меж інтервалів $[\,\delta y_i^-,\delta y_i^+\,]$ відхилень вихідної характеристики від номінального значення, відповідно;

$\tilde{F}=\{\phi_{ij}, i=\overline{1,N}, j=\overline{1,m}\}$ – відома матриця значень похідних функцій $g_i(\vec{b})$ у точці $\vec{b}_0$;

$\delta\vec{b}=(\delta b_1,...,\delta b_m)^T$ – вектор відхилень значень параметрів від номінального.

Зауважимо, що коефіцієнти ϕ_{ij} задають чутливості i-ої вихідної характеристики до зміни j-го параметра b_j.

Розв'язком інтервальної системи лінійних алгебраїчних рівнянь (1) є множина допустимих відхилень параметрів від номінальних значень. Позначимо цю множину як $\tilde{\Omega}$. У просторі параметрів вона є опуклим многогранником. Будь-які відхилення $\delta\vec{b}$ параметрів, $\vec{b}$ вибрані із множини $\tilde{\Omega}$, забезпечують допустимі відхилення усіх виходів y_i.

Розрахунок допустимих відхилень параметрів системи вимагає знаходження їх значень на основі множини $\tilde{\Omega}$ у такий спосіб, щоб забезпечити задану імовірність працездатності.

Метод допустимого оцінювання

Враховуючи властивості допустимої області параметрів, заданої системою інтервальних рівнянь (1), оцінювання допусків для заданого рівня функціональної придатності здійснюватимемо на основі процедури зіставлення допустимої області $\tilde{\Omega}$ із технологічною областю розсіювання значень відхилень за умови нормального закону їх розподілу.

Під час розгляду системи інтервальних рівнянь (1) для випадку $N = m$ вважатимемо, що матриця $\tilde{F}$ є не виродженою, тобто $det(\tilde{F}) \neq 0$, $rang(\tilde{F}) = m$. Тоді розв'язком системи (1) є множина $\tilde{\Omega}_m$, яка в просторі параметрів визначає m-вимірний паралелепіпед із вершинами $\delta\vec{b}_s$:

$$\delta\vec{b}_s = \tilde{F}^{-1} \cdot \delta\vec{Y}_s \ , \ \ s = 1,...,2^m \ , \tag{2}$$

де $\delta\vec{Y}_s$ – вектор, складений із комбінацій нижніх та верхніх меж інтервалів $[\delta y_i^-, \delta y_i^+]$ відхилень вихідної характеристики від номінального значення.

Шукатимемо допустиму оцінку, отриманої множини $\tilde{\Omega}_m$, у класі еліпсоїдних множин Q_m^- максимального об'єму із розв'язку такої задачі:

$$V(Q_m^-) \xrightarrow{Q_m^-} max \ , \ Q_m^- \subset \tilde{\Omega}_m \ , \tag{3}$$

де $V(Q_m^-)$ – об'єм допустимого еліпсоїда.

Очевидно, що завдяки симетрії m-вимірного паралелепіпеда $\tilde{\Omega}_m$, допустимий (вписаний) еліпсоїд Q_m^- максимального об'єму повинен дотикатися до усіх його граней.

Задача (3) є достатньо складною задачею математичного програмування. Однак, користуючись властивостями множини $\tilde{\Omega}_m$, загальний розв'язок цієї задачі можна отримати в аналітичному вигляді.

Результати, наведені в [2], показують, що для випадку, коли кількість невідомих характеристик N збігається з кількістю невідомих параметрів m, допустима область Ω_m може бути наближена допустимим оптимальним (максимальним об'ємом) m-вимірним еліпсоїдом

$$Q_m^- = \left\{ \delta\vec{b} \in R^m \middle| \ (\delta\vec{b} - \delta\vec{\bar{b}})^T \cdot \tilde{F}^T \cdot \tilde{E}^{-2} \cdot \tilde{F} \cdot (\delta\vec{b} - \delta\vec{\bar{b}}) \leq 1 \right\}, \tag{4}$$

тобто таким, що дотикається до центрів усіх граней, і з центром ваги

$$\delta\vec{\bar{b}} = \tilde{F}^{-1} \cdot \delta\vec{\bar{Y}} \ .$$

У виразі (4) $\tilde{E}$ – діагональна матриця допусків $\tilde{\Delta}_i = 0{,}5 \cdot (\delta y_i^+ - \delta y_i^-)$, $i = 1,...,m$ відхилень вихідних характеристик статичної системи. Вектор $\delta\vec{\bar{Y}}$ має такий вигляд:

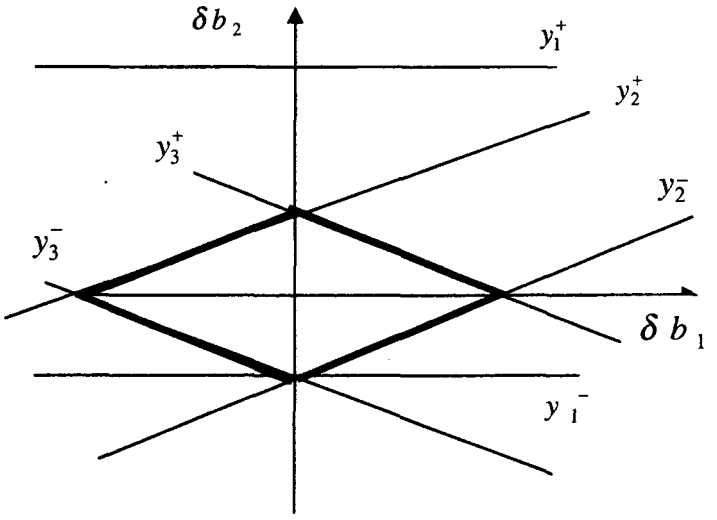
$$\delta\vec{\bar{Y}} = (\delta\bar{y}_1,...,\delta\bar{y}_i,...,\delta\bar{y}_m)^T \ , \ \delta\bar{y}_i = 0{,}5 \cdot (\delta y_i^+ + \delta y_i^-) \ .$$

Якщо ж кількість характеристик системи перевищує кількість параметрів $N > m$, то в цьому випадку використовується наближення отримання допустимої області у вигляді m-вимірного паралелепіпеда (рисунок) для $m = 2$.

У разі $N < m$ для отримання наближення допустимої області у вигляді m-вимірного паралелепіпеда система інтервальних рівнянь (1) довизначається такими рівняннями:

$$\delta b_j^- \leq \delta b_j \leq \delta b_j^+ \ . \tag{5}$$

Отже, для будь-якого із випадків $N = m$, $N > m$, $N < m$ є можливість подати допустиму область у вигляді m-вимірного паралелепіпеда і відповідного допустимого еліпсоїда (4).



Розглянемо випадок, коли випадкові відхилення δb_j параметрів розподілені за нормальним законом. В цьому випадку допуски для відхилень δb_j параметрів системи задають довірчими інтервалами:

$$-\vec{\sigma}\cdot u(\alpha)\le\delta\vec{b}\le\vec{\sigma}\cdot u(\alpha), \tag{6}$$

де $\vec{\sigma}=(\sigma_1,...,\sigma_m)^T$ – вектор відомих стандартних відхилень параметрів системи; $u(\alpha)$ – табличне значення (квантиль) нормованого нормального закону розподілу; α – довірча імовірність.

Знайдемо допустимі дисперсії технологічних відхилень за заданої імовірності працездатності $P=1-\alpha$ системи на межі області, яка задається у вигляді еліпсоїда. З цією метою підставимо у формулу (4) замість δb вектор довірчих інтервалів $[-\vec{\sigma}\cdot u(\alpha);\vec{\sigma}\cdot u(\alpha)]$ для квантиля $u(\alpha)$ і отримаємо

$$u^2(\alpha)\cdot[\vec{\sigma}^T]\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot[\vec{\sigma}]-2\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot[\vec{\sigma}]-,$$

$$\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\delta\vec{\vec{b}}=1. \tag{7}$$

Рівняння (7) є квадратним інтервальним рівнянням з невідомими інтервальними дисперсіями параметрів $\vec{\sigma}$. Задаючи співвідношення між дисперсіями параметрів за допомогою вектора коефіцієнтів $\vec{k}=(k_1,\cdots,k_m)^T$ у вигляді $[\vec{\sigma}]=[\sigma]\cdot\vec{k}$ і підставляючи їх у рівняння (7), отримаємо

$$[\sigma]^2\cdot u^2(\alpha)\cdot\vec{k}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}-2\cdot[\sigma]\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}-,$$

$$\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\delta\vec{\vec{b}}=1. \tag{8}$$

Розв'язками рівняння (8) є інтервали $[-\sigma_1;\sigma_1]$, $[-\sigma_2;\sigma_2]$,

де

$$\sigma_1=(2\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}+((2\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k})^2-4\cdot u^2(\alpha)\cdot\vec{k}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}\cdot$$
$$\cdot(\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\delta\vec{\vec{b}}-1))^{1/2})/2\cdot u^2(\alpha)\cdot\vec{k}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k};$$

$$\sigma_2=(2\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}+((2\cdot u(\alpha)\cdot\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k})^2+4\cdot u^2(\alpha)\cdot\vec{k}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}\cdot$$
$$\cdot(\delta\vec{\vec{b}}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\delta\vec{\vec{b}}-1))^{1/2})/2\cdot u^2(\alpha)\cdot\vec{k}^T\cdot S^T\cdot\tilde{E}^{-2}\cdot S\cdot\vec{k}.$$

Допустиме значення дисперсії знаходимо із виразів $\sigma^-=max\{-\sigma_1,-\sigma_2\}$; $\sigma^+=min\{\sigma_1,\sigma_2\}$, а формула для розрахунку допустимих значень параметрів, що забезпечують імовірність працездатності системи не нижче $P=1-\alpha$, матиме вигляд

$$[\delta b_j^-;\delta b_j^+]=[k_j\cdot\sigma^-,k_j\cdot\sigma^+],\ j=1,...,m.$$

Варто зауважити, якщо центр $\vec{\delta b}$ еліпсоїда дорівнює нульовому вектору $\vec{\delta b} = (0,...,0)^T$, то рівняння (8) істотно спрощується і набуває такого вигляду:

$$[\sigma]^2 \cdot u^2(\alpha) \cdot \vec{k}^T \cdot S^T \cdot \tilde{E}^{-2} \cdot S \cdot \vec{k} = 1, \qquad (9)$$

а для розрахунку $[\sigma]$ використовуємо формулу

$$[\sigma] = 1/\sqrt{u^2(\alpha) \cdot \vec{k}^T \cdot S^T \cdot E^{-2} \cdot S \cdot \vec{k}}\,.$$

Розроблений метод передбачається використати для оцінювання допустимих значень характеристик підсистем електрогенеруючих систем та систем електропостачання.

Необхідно зазначити, що запропонований метод допустимого оцінювання вимагає подальшого розвитку в напрямку автоматичного формування вектора $\vec{k} = (k_1,\cdots,k_m)^T$, що задає співвідношення між дисперсіями параметрів, на основі критерію максимізації допустимої області.

Висновки

1. На основі аналізу існуючих методів допустимого оцінювання параметрів статичних багатоелементних систем обґрунтоване застосування для цих цілей методів інтервального аналізу, які дають змогу отримати оцінки допустимої області у вигляді багатовимірних еліпсоїдів.

2. Використання еліпсоїдних оцінок допустимої області параметрів уможливило розробити метод оцінювання допустимих значень параметрів підсистем складних систем, який на відміну від існуючих, дає змогу отримати аналітичний розв'язок під час забезпечення заданої імовірності працездатності системи загалом.

1. Дивак М.П. Допустиме оцінювання області параметрів радіоелектронних кіл в класі еліпсоїдів // Теоретична електротехніка. – 2002. – Вып. № 56 – С. 113–122. 2. Дивак М.П., Франко Ю.П. Методи аналізу інтервальних даних стосовно оцінки технологічних процесів виготовлення інтегральних схем // Теоретична електротехніка. – 2000. – Вып. 55. – С. 167–173. 3. Кривошейкин А.В. Точность параметров и настройка аналоговых радиоэлектронных цепей. – М., 1983.

УДК 621.372

П.І. Чопик[1], Б.П. Русин[2]

[1]Тернопільський національний педагогічний університет ім. В. Гнатюка,
[2]Фізико-механічний інститут ім. Г.В. Карпенка НАН України

МЕТОДИ ВІДНОВЛЕННЯ ТРИВИМІРНОЇ ФОРМИ ОБ'ЄКТІВ ЗА МЕТАЛОГРАФІЧНИМИ ЗОБРАЖЕННЯМИ

Вибрано метод для відновлення тривимірної форми реальних об'єктів. Розглянуто найпоширеніші методи: із стереозображення, за даними про півтони, за відображенням руху.

The choice of method is the purpose of the article for renewal of three-dimensional form of the real objects. The most widespread methods are considered: shape from stereo, shape from shading, structure from motion.

Постановка проблеми

Інтерес до методів відновлення тривимірної структури сцен за їх плоскими зображеннями відновився в середині XX ст. у зв'язку з дослідженнями в області штучного інтелекту, а практична потреба в робототехнічних пристроях, здатних орієнтуватися в тривимірному просторі, постійно