Литература :

1. Демидович Б.П. Лекции по математической теории устойчивости. – М., 1998. – 480 с.

2. Tonkov E.L. Uniform attainability and Lyapunov reducibility of bilinear control system // Proceedings of the Steklov Institute of Mathematics. – Suppl. 1. 2000. – P. S228-S253.

3. Макаров Е.К., Попова С.Н. О глобальной управляемости полной совокупности ляпуновских инвариантов двумерных линейных систем // Дифференц. уравнения. – 1999. – Т. 35, № 1. – С. 97–106.

УДК 517.926

Влияние выбора аппроксимации обобщенных коэффициентов на решения линейных дифференциальных уравнений

Капусто А.В.
Белорусский национальный технический университет

Решение проблемы умножения обобщенных функций стало возможным после построения более широкого пространства – новых обобщенных функций, – для которого определена операция умножения и вложение пространства обобщенных функций. Общий метод построения новых алгебр обобщенных функций, а также анализ наиболее известных конструкций Коломбо и Егорова, был представлен в работе Антоневича А.Б. и Радыно Я.В. [1]. По своему построению новые обобщенные функции сохраняют информацию о способе получения их из гладких, т.е. «помнят свое происхождение», поэтому было предложено называть их мнемофункциями. Как одна из модификаций конструкции Коломбо, было построено пространство мнемофункций $G(\mathbb{R})$ [2] .

Заметим, что при вложении пространства обобщенных функций $D'(\mathbb{R})$ в $G(\mathbb{R})$ каждой обобщенной функции соответствует бесконечно много мнемофункций. Например, есть много разных мнемофункций, ассоциированных с $\delta-$функцией, также как и много разных функций ассоциированных с нулем. Данная особенность приводит к тому, что решения дифференциальных уравнений, полученные для таких мнемофункций, могут соответствовать разным обобщенным функциям. Исследования в пространстве $G(\mathbb{R})$ позволили получить новые свойства и эффекты решения задачи Коши уже для линейного дифференциального уравнения первого порядка с обобщенными коэффициентами: неединственность решения задачи Коши, слипание решений, возможность продолжения решения через особую точку. В настоящее время ведутся

исследования по увеличению класса примеров решения линейных дифференциальных уравнений с $\delta-$образными коэффициентами и свободными членами, а также влияния на решения постоянных слагаемых в коэффициентах, ассоциированных с нулем.

Литература:

1. Антоневич, А.Б. Об общем методе построения алгебр обобщенных функций / А.Б. Антоневич, Я.В. Радыно // Докл. АН СССР. – 1991. – Т.312, № 2. – С. 267-270.

2. Антоневич, А.Б. Линейные дифференциальные уравнения с обобщенными коэффициентами с точки зрения мнемофункций / А.Б. Антоневич, А.В. Турло // Дифференц. уравнения. – 1994. – Т.30, № 5. – С. 758-767.

УДК003.26:51:004(075.8)

Полиномиальные кольца классов вычетов в защите информации

Королева М.Н., Липницкий В.А.
Белорусский национальный технический университет

Пусть $\mathbb{Z}_p$ – кольцо классов вычетов по модулю простого числа, пусть $\mathbb{Z}_p[x]$ – кольцо полиномов с коэффициентами из $\mathbb{Z}_p$. Зафиксируем натуральное число $n>1$. В помехоустойчивом кодировании основополагающую роль играет фактор-кольцо $R_n=\mathbb{Z}_p[x]/<\mathrm{x}^n-1>$ кольца $\mathbb{Z}_p[x]$ по идеалу $<\mathrm{x}^n-1>$, порожденному полиномом x^n-1. Идеалы кольца R_n интерпретируются как циклические коды длиной n, определённые над полем Галуа $\mathbb{Z}_p$ (как правило, $p=2$). Как и в кольце $\mathbb{Z}_p[x]$, все идеалы кольца R_n являются главными: в каждом собственном идеале $J\subset R_n$ найдется полином $m(x)\neq 0$ наименьшей степени, тогда $J=<m(x)>-$ совпадает с главным идеалом, порожденным полиномом $m(x)$. Поскольку всякий собственный идеал любого кольца состоит из необратимых элементов этого кольца, полином $m(x)$ неизбежно обязан быть делителем полинома x^n-1.

В 1994 г. была создана криптосистемы NTRU именно на основе кольца R_n. Её циклические коды порождаются делителями x^n-1, принадлежащими классу круговых полиномов. NTRU использует в