Поясним, почему так происходит, используя упрощенный числовой пример. Пусть мы сравниваем одинаково отличающиеся объекты, площадь шести кругов. Будем считать, что с точки зрения эксперта площадь первого круга равна единице, площадь второго больше в два раза, площадь третьего больше в четыре раза и так далее. Тогда получим следующую последовательность значений для площади круга:

1, 2, 2^2, 2^3, 2^4, 2^5. (1)

Конечно, мы можем сравнивать не только рядом стоящие пары объектов.

Чтобы быть адекватным, эксперт должен бы ответить, что третий круг на два порядка больше первого (2^2), а четвертый круг на три порядка (2^3) больше первого.

На самом деле, когда Стивенс просил своих испытуемых сообщать во сколько раз одно ощущение больше другого, то испытуемый делал то, что он может делать - оценивал величину объекта в порядковой шкале и сообщал отношение рейтингов объектов, а не размеров. Например, что второй круг в два раза больше первого, третий в три раза больше первого и так далее. В этом случае последовательность субъективных оценок площади

1, 2, 3, 4, 5, 6. (2)

Оценки (1) – сроятся на основании рейтинга объектов, оценки (2) являются рейтингом объектов. Оценки (2) соответствуют закону Стивенса, оценки (1) – модели нефизического измерения величины.

Модель нефизического измерения можно использовать для характеристики вероятности, полезности или качества объектов.

УДК 530.182

РЕШЕНИЯ ТИПА WOBBLING KINK И OSCILLATING KINK В ТЕОРИИ ϕ^4

Князев М.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Значительный интерес к скалярной модели ϕ^4 обусловлен её широким использованием для описания нелинейных процессов и явлений во многих областях физики. В (1+1)-мерном случае плотность функции Лагранжа модели имеет вид

$$\mathcal{L}(x,t) = \frac{1}{2}\left(\dot{\phi}\right)^2 - \frac{1}{2}(\phi')^2 - \frac{1}{4}\lambda\left(\phi^2 - \frac{m^2}{\lambda}\right)^2,$$

где m – масса поля, λ – постоянная связи; точка соответствует дифференцированию по времени, а штрих – по пространственной координате. Уравнение движения модели записывается в виде [1]

$$\ddot{\phi} - \phi'' = m^2\phi - \lambda\phi^3 . \quad (1)$$

Данное уравнение относится к классу неинтегрируемых существенно нелинейных уравнений в частных производных [2] и для него можно построить только одно топологически нетривиальное солитоноподобное решение. Оно называется одиночным кинком (антикинком) и имеет вид

$$\phi = \pm\frac{m}{\sqrt{\lambda}}\tanh\left[\frac{m}{\sqrt{\lambda}}\left(\frac{x-x_0-ut}{\sqrt{1-u^2}}\right)\right], \quad (2)$$

где "+" соответствует кинку, а "–" – антикинку; x_0 характеризует положение решения в начальный момент времени.

Наряду с точным решением (2) уравнение (1) допускает существование и ряда других приближенных решений. Особый интерес среди таких приближенных решений представляют решения, для которых характерна периодическая зависимость от времени. Наиболее известны из них это решения типа oscillating kink и wobbling kink. Несмотря на периодическую зависимость обоих решений от времени, характер этой зависимости позволяет различать их в принципе.

Важным свойством кинков (и вообще, любых солитонов или солитоноподобных объектов) считалась их способность сохранять форму в процессе взаимодействия. Численные эксперименты показывали, что единственное отличие между двумя кинками (антикинками, кинком и антикинком) в результате их столкновения заключается в появлении дополнительного сдвига фазы между такими решениями. Это позволяло надеяться на возможность использования этих решений для описания упругих столкновений элементарных частиц. Дальнейшие исследования, однако, привели к двум важным результатам.

Первый из них состоит в том, что не всегда кинки (и антикинки) не сохраняют форму в процессе взаимодействия. После взаимодействия они восстанавливают ту форму, которой обладали до взаимодействия. В самом процессе же взаимодействия их форма может изменяться, причем весьма существенно. Эти изменения, как правило, носят характер нерегулярных колебаний с переменными амплитудой и частотой, которые в дальнейшем, в соответствии с общепринятой практикой, мы будем называть осцилляциями. Характер этих осцилляций зависит не только от значений параметров модели, но и от того, какие механизмы взаимодействия в модели учитываются. В случае кинков подобного рода решения в англоязычной литературе называются oscillating kink.

К первым работам, в которых появляются колебательные процессы применительно к кинкам, можно отнести статьи [3, 4], посвященные возможности существования связанного состояния

кинк-антикинк. По аналогии с теорией sin-Гордон такое состояние называется бризером. В работе [3] предпринята попытка численного решения уравнения (1), с целью построить решение, описывающее бризер в теории ϕ^4. Было показано, что для уравнения (1) можно приближенно построить локализованное слабозатухающее решение, которое медленно осциллирует во времени. Это решение не является точным и для него не удалось получить замкнутое аналитическое выражение.

Похожая ситуация имеет место и в работе [4], в которой также рассматривается проблема связанных состояний кинков. Показано, что в установившемся режиме возникает квази-связанное состояние двух кинков, которое характеризуется регулярными колебаниями. Найдено приближенное аналитическое выражение для этого состояния.

Осцилляции решений в обеих работах обусловлены процессами диссипации энергии при взаимодействии кинков. В настоящее время доказано, что бризер в теории ϕ^4 не существует [5]. Для уравнения (1) возможно только формальное асимптотическое представление для бризера в пределе малых амплитуд и частот. Силы взаимодействия между решениями, составляющими бризер, не только сложным образом зависят от положения этих составляющих, но и неустойчивы по отношению к расстоянию между ними. Вследствие постоянного излучения энергии бризер очень быстро распадается.

Однако, как следует из работы [6], уравнение (1) может иметь осциллирующие решения, и не только соответствующие связанным состояниям, если учесть дополнительные механизмы переноса энергии. Эти механизмы могут описывать как внутренние свойства системы, тогда их вклады можно учесть в выражении для потенциала, так и внешнее воздействие, тогда уравнение (1) будет неоднородным.

В указанных выше примерах колебания носили произвольный характер с широкими диапазонами изменений амплитуды и частоты.

Во-вторых, оказалось, что, если нелинейное уравнение имеет статическое решение в виде кинка (солитона или какого-либо солитоноподобного объекта), то для такого уравнения могут существовать решения особого типа, которые обладают дополнительной внутренней степенью свободы. Для таких решений среднее по времени значение удовлетворяет граничным условиям для обычных решений, но в тоже время само решение является периодической функцией координат и времени. Периодический характер такого решения также можно связать с тем, что профиль функции является осциллирующим. Однако, как следует из результатов вычислений, данные осцилляции носят особый характер. Их величина определяется параметром порядка системы, который значительно меньше её характерного размера. Таким образом, эти осцилляции представляют собой нечто похожее на дрожание вещества в студенистом состоянии. Для таких кинков в англоязычной литературе принято название wobbling kink. Можно сказать, что по сравнению с обычным кинком wobbling kink обладает своего рода «тонкой» структурой.

Впервые проблема состояний нелинейной системы, для описания которых в настоящее время используются решения в виде колеблющегося кинка, была описана при экспериментальном исследовании пиннинга (зацепления дислокаций) в полиацетилене $(CH)_x$ [7].

Наиболее подробно теория решений типа wobbling kink разработана в работе [8]. Эту работу можно рассматривать как основополагающую в теории таких решений. В ней показано, что, если нелинейное уравнение в частных производных допускает точное решение в виде статического кинка, то оно также будет иметь, по крайней мере приближенное, решение в виде wobbling kink. Такое новое решение удовлетворяет граничным условиям для обычного кинка, но является периодической функцией времени. Это становится возможным благодаря дополнительной внутренней степени свободы состояния. Разработан формальный метод построения аналитических выражений для wobbling kinks в моделях ϕ^4 и sine-Gordon в виде степенных рядов. При этом анзац решения выбирается в таком виде, чтобы члены ряда сразу были бы равномерно ограниченными функциями по времени, а надо вычислить пространственные сомножители в таком виде, чтобы и они были равномерно ограниченными функциями, но уже по пространственной координате. Доказано, что такого рода ряды являются асимптотическими, если рассматривать достаточно большие промежутки времени. Основное предположение физического характера при данном подходе состоит в том, что wobbling kink представляется в виде суперпозиции линейных осцилляторов. Однако, как показывают дополнительные исследование, такое приближение носит ограниченный характер и пригодно только для нескольких первых членов ряда (в зависимости от модели). Если же попытаться вычислить члены более высоких порядков вышеупомянутого асимптотического ряда, то они перестают быть равномерно ограниченными и ряд расходится. Это связано с тем, что по сути дела колебания носят нелинейный характер и эта нелинейность становится существенной. Особенностью нелинейного осциллятора является зависимость амплитуды от частоты, и, если для первых членов ряда эта зависимость не столь значительна, то в дальнейших расчетах ею уже пренебрегать нельзя.

1. Раджараман, Р. Солитоны и инстантоны в квантовой теории поля / Р. Раджараман. – М.: Мир, 1985. – 416 с.

2. Абловиц, М. Солитоны и метод обратной задачи / М. Абловиц, Х. Сигур – М.: Мир, 1987. – 479 с.
3. Кудрявцев, А.Е. О солитоноподобных решениях для скалярного поля Хиггса / А.Е. Кудрявцев // Письма в ЖЭТФ – 1975. – Т. 22, вып. 3. – С. 178-181.
4. Гетманов. Б.С. Связанные состояния солитонов в моделях теории поля ϕ_2^4 / Б.С. Гетманов // Письма в ЖЭТФ – 1976. – Т. 24, вып. 5. – С. 323-327.
5. Segur, H. Nonexistence of small-amplitude breather solutions in ϕ^4 theory / H. Segur, M.D. Kruskal // Phys. Rev. Lett. – 1987 – V. 58, № 8. – P. 747-750.
6. Лидский, Б.В. Периодические решения уравнения $u_{tt} - u_{xx} + u^3 = 0$ / Б.В. Лидский, Е.И. Шульман // Функциональный анализ и его приложения – 1988 – Т. 22. Вып. 4. – С. 88-89.
7. Rice, M.J. Charge Π-phase kinks in lightly doped polyacetilene / M.J. Rice // Phys. Lett. A. – 1979 – V. 71, № 1. – P. 152-154.
8. Segur, H. Wobbling kink in ϕ^4 and sine-Gordon theory / H. Segur // J. of Math. Physics – 1983. – V. 24, № 6. – P. 1439-1443.

УДК 512.624.95:378.147.091.3

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ КРИПТОСИСТЕМЫ РАБИНА

Крупенкова Т.Г.[1], Липницкий В.А.[2]
[1]Белорусский национальный технический университет, Минск, Республика Беларусь
[2]Военная академия Республики Беларусь, Минск, Республика Беларусь

Криптосистема Рабина явилась результатом переосмысления криптосистемы RSA. Рабин М. заинтересовался вопросом выбора ключа e в криптосистеме RSA. Там e всегда взаимно просто с $\varphi(n)$ и, в частности, всегда нечётно. А что произойдёт, если взять чётным? Да, а если возьмём наипростейший случай $e = 2$? В результате подробного рассмотрения неожиданно и появилась рассматриваемая здесь криптосистема Рабина.

Пусть p и q – два различных простых числа. Пусть $N = pq$. Зафиксируем число B, $0 \le B < N$. Пара $\{N, B\}$ есть пара открытых ключей криптосистемы Рабина. Сообщение C рассматривается как элемент кольца Z/NZ и шифруется формулой: $m = c(c + B) (\mathrm{mod} N)$. Ясно, что такой способ шифрования реализуется гораздо быстрее, чем в криптосистеме RSA.

Расшифровка здесь представляет гораздо более сложную процедуру даже для законного получателя криптотекста. Фактически, сообщение C есть один из корней квадратного уравнения $x^2 + Bx - m = 0$ в кольце Z/NZ. В этом кольце 2, очевидно, является обратимым элементом. Поэтому для решения данного квадратного уравнения вполне пригодны стандартные формулы: $x = (\sqrt{\frac{B^2}{4} + m} - \frac{B}{2}) \ (\mathrm{mod} N)$. Разумеется, деление на 2 здесь реализуется умножением на $2^{-1} \in Z/NZ^*$. Сложность этих вычислений в том, что из каждого квадрата в данном кольце Z/NZ извлекаются 4 различных корня.

Другая проблема – как найти быстро квадратные корни из данного элемента кольца Z/NZ – в общем случае остаётся открытой. Существенно облегчает её решение знание делителей числа N. Тогда можно воспользоваться китайской теоремой об остатках и формулой Гарнера. Поэтому сложность взлома криптосистемы Рабина такая же, как и криптосистемы RSA.

Если разложение $n = p \cdot q$ в произведение простых множителей p и q известно, то легко находится CRT-представление дискриминанта: $D \leftrightarrow (D_p, D_q)$. Квадратный корень из D извлекается в Z/nZ, тогда и только тогда, когда D принадлежит подгруппе квадратов Z/nZ^{*2} в группе Z/nZ^*. А это возможно тогда и только тогда, когда $D_p \in Z/pZ^{*2}$ и $D_q \in Z/qZ^{*2}$. Проверить это, а заодно и найти корни можно, в принципе, прямым перебором: вычисляем по модулю p последовательно 2^2, 3^2, и так далее, пока не найдём эмпирически $u \le (p\ 1)$, такое, что $u^2 (\mathrm{mod} p) \equiv D_p$. Аналогично поступаем с D_q.

В трёх из четырёх случаев теория чисел даёт прямые формулы для квадратных корней из нечётных простых чисел, то есть решает проблему поиска квадратных корней.

Следует напомнить, что для всех простых p кольцо Z/pZ является полем. Классическая теория полиномов справедлива для всех полей. В частности, имеет место однозначность разложения всякого полинома в произведение неприводимых полиномов-сомножителей. Отсюда следует, что каждый полином степени $n \ge 1$ с коэффициентами из Z/pZ имеет не более n корней. В частности, полином $x^2 - \overline{1}$ имеет в точности два корня: $\overline{1}$ и $\overline{-1}$.

Проблема поиска квадратных корней остаётся открытой для полей Z/pZ с нечётными простыми $p \equiv 1 (\mathrm{mod} 8)$. В этом случае прямых формул не существует, но есть вполне детерминированный процесс нахождения квадратных корней. Здесь $p - 1 = 2^e \cdot q$, где $e \ge 3$, q – нечётное число. Циклическая группа Z/pZ^* содержит единственную циклическую подгруппу G порядка 2^e. Пусть f – квадратичный невычет по модулю p из множества