УРАВНЕНИЕ ТЕПЛОПРОВОДНОСТИ НА БУЛЕВОМ КУБЕ

В.А. Волошко

Белгосуниверситет, НИИ прикладных проблем математики и информатики, Минск, Беларусь
ValeraVoloshko@yandex.ru

Рассмотрим уравнение теплопроводности:

$$\frac{d}{dt}f(t,x) = \Delta_x f(t,x), \tag{1}$$

где Δ — лапласиан. Это одно из фундаментальных уравнений математики с хорошо известными классическими приложениями и интерпретациями. В частности, (1) описывает случайные блуждания и процессы распространения (диффузии). Здесь предлагается еще одна интерпретация.

Функция f в (1) зависит от двух переменных — временной t и пространственной x. В классическом случае время и пространство непрерывны. Рассмотрим дискретное пространство, а именно булев куб $\{0,1\}^n$ со стандартным лапласианом $\Delta\phi(x) = \sum_y \phi(y) - n\phi(x)$, где суммирование ведется по $y \in \{0,1\}^n$, отличным от x в одной позиции. Тогда $f(t,\cdot)$, будучи в момент $t \in \mathbb{R}$ вероятностной мерой — неотрицательной с единичной суммой по пространству — остается таковой и в будущем. Более того, (1) сохраняет единичную сумму по пространству вдоль всей временной оси — в

будущем и в прошлом. Поэтому неотрицательность — единственное свойство вероятностной меры, которое может быть потеряно в прошлом. Момент, когда это происходит, представляет определенный прикладной интерес. Удаленность этого момента от настоящего назовем *натуральным временем диффузии* и определим как

$$\mathbf{T}(\phi) ::= -\inf\{t \in \mathbb{R} : f(t,x) \geqslant 0, \quad \forall x \in \{0,1\}^n\} \geqslant 0, \tag{2}$$

где $\phi(x) = f(0,x)$ — исходная вероятностная мера при $t = 0$ в (1). Слово «натуральный» в названии для (2) указывает на отсутствие коэффициента при лапласиане в (1).

Определение (2) вообще говоря никак не привязано к булеву кубу и корректно для любого пространства, снабженного лапласианом. Но для булева куба уравнение теплопроводности (1) и натуральное время диффузии (2) имеют простую ясную интерпретацию, связанную с двоичными данными и близкими темами, такими как криптография и стеганография. А именно, рассмотрим следующую очень распространенную модель: $\xi \in \{0,1\}^n$ — случайное двоичное ϕ-распределенное n-слово, представимое в виде $\xi = \zeta \oplus \eta$, где ζ и η — независимые случайные двоичные n-слова, $\oplus$ — поэлементная сумма по модулю 2, и η состоит из n независимых бернуллиевских случайных величин с вероятностями успеха $\mathbb{P}\{\eta_i = 1\} = \varepsilon$. Тогда (2) определяет, насколько ε может быть близким к $1/2$:

$$|\varepsilon - 1/2| \geqslant e^{-\mathbf{T}(\phi)}/2.$$

Эта граница имеет значение, к примеру, в стеганографии, где используется стандартная модель вкрапления равномерно распределенной последовательности в двоичный контейнер [1, 2]. В [1] для такой модели вкрапления был построен алгоритм корректировки заполненного контейнера, сохраняющий встроенную информацию и восстанавливающий частоты подслов. Емкость контейнера — предельно допустимая доля вкрапления, допускающая корректировку — равна $1 - e^{-\mathbf{T}(\phi)}$, где ϕ — вероятностная мера, отвечающая подсловам контейнера.

Литература

1. Волошко В. А. *Стеганографическая емкость одномерного марковского контейнера* // Дискретная математика. 2016. Т. 28, № 1. С. 19–43.

2. Харин Ю. С., Вечерко Е. В. *Распознавание вкраплений в двоичную цепь Маркова* // Дискретная математика. 2015. Т. 27, № 3. С. 123–144.