

Московский государственный технический университет
имени Н.Э. Баумана

Д.А. Жуков, П.Г. Ключарев

ИЗБРАННЫЕ ЗАДАЧИ ПРИКЛАДНОЙ ДИСКРЕТНОЙ ГЕОМЕТРИИ

*Рекомендовано Научно-методическим советом
МГТУ им. Н.Э. Баумана
в качестве учебного пособия*

Москва
Издательство МГТУ им. Н.Э. Баумана
2012

УДК 519.1(075.8)

ББК 22.176

Ж86

Рецензенты: *А.Н. Велигура, А.Ю. Голубков*

Жуков Д. А.

Ж86 Избранные задачи прикладной дискретной геометрии : учеб. пособие / Д. А. Жуков, П. Г. Ключарев. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2012. — 53, [3] с. : ил.

Рассмотрены алгебраические и комбинаторные свойства различных подмножеств булева куба, нашедшие применение в теории булевых функций, теории сложности, защите информации и теории кодирования. Приведены задачи с подробными решениями и упражнения различной степени сложности, предназначенные как для первоначального, так и для углубленного освоения методов дискретной математики и комбинаторного анализа.

Для студентов первого курса, обучающихся специальностям «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем».

Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00508).

УДК 519.1(075.8)

ББК 22.176

Учебное издание

Жуков Дмитрий Александрович

Ключарев Петр Георгиевич

ИЗБРАННЫЕ ЗАДАЧИ ПРИКЛАДНОЙ ДИСКРЕТНОЙ ГЕОМЕТРИИ

Редактор *О.М. Королева*

Корректор *О.В. Калашиникова*

Компьютерная верстка *В.И. Товстоног*

Подписано в печать 05.07.2012. Формат 60×84/16.

Усл. печ. л. 3,26. Тираж 100 экз. Изд. № 47.

Заказ

Издательство МГТУ им. Н.Э. Баумана.

Типография МГТУ им. Н.Э. Баумана.

105005, Москва, 2-я Бауманская ул., 5.

© МГТУ им. Н.Э. Баумана, 2012

ВВЕДЕНИЕ

При изучении дискретной математики и программирования часто приходится сталкиваться с вопросами существования, генерирования и подсчета числа различных комбинаторных объектов. Одним из наиболее замечательных объектов комбинаторики является многомерный булев куб. Комбинаторные свойства булева куба находят многочисленные приложения при передаче и защите информации, в дискретной геометрии и теории алгоритмов, в теории графов и комбинаторном анализе, в теории булевых функций и параллельных вычислениях и с развитием этих дисциплин становятся неотъемлемой частью обязательных университетских курсов.

Авторами пособия сделана попытка, не претендуя на полноту охвата материала, показать связь комбинаторики булева куба с другими разделами дискретной математики, чтобы облегчить переход студентов к ее углубленному изучению на старших курсах. На многочисленных примерах разобраны метрические свойства подмножеств булева куба, рассмотрены код Хемминга и код Грея, доказана теорема Шпернера. Все примеры в тексте снабжены подробными решениями, а в конце пособия приведено несколько задач для самостоятельного решения.

Углубленные сведения о предмете можно найти в работах [1 — 14].

Авторы рассчитывают, что читатель знает элементарные понятия комбинаторики и алгебры в пределах первого семестра, и рекомендуют обратиться к учебникам [1, 2, 3] в случае затруднений.

В пособии использованы стандартные обозначения: $\mathbb{N} = \{1, 2, \dots\}$ — множество натуральных чисел; $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

— множество целых чисел; $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ — множество вычетов по модулю m ; $\mathbb{R}$ — множество действительных чисел; $A^m = A \times \dots \times A$ — декартова степень множества A ; $|A|$ — его мощность (число элементов).

1. БУЛЕВ КУБ КАК МЕТРИЧЕСКОЕ ПРОСТРАНСТВО

Множество $\mathbb{Z}_2^n = \{0, 1\}^n = \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$, состоящее из всех упорядоченных наборов нулей и единиц длины n , называется *булевым кубом размерности n* . Его элементы — двоичные наборы — будем обозначать греческими буквами: $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}, \dots$. В качестве примера приведем список всех двоичных наборов длины три:

$$\mathbb{Z}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Наборы в этом списке идут в так называемом *лексикографическом* порядке, т. е. в порядке следования всех трехбуквенных слов в словаре слов двухбуквенного алфавита (0 — первая буква этого алфавита, 1 — вторая). Очевидно, что $|\mathbb{Z}_2^n| = 2^n$ при всех $n \in \mathbb{N}$.

Пусть X — произвольное множество и $\rho : X \times X \mapsto \mathbb{R}$ — некоторая функция, определенная на упорядоченных парах элементов множества X и принимающая действительные значения. Функция ρ называется *метрикой*, или *расстоянием*, на множестве X , если она удовлетворяет трем свойствам, которые называются *аксиомами метрики*:

- 1) симметричность: $\forall x, y \in X \quad \rho(x, y) = \rho(y, x)$;
- 2) неотрицательность: $\forall x, y \in X \quad \rho(x, y) \geq 0$, причем $\rho(x, y) = 0 \Leftrightarrow x = y$;
- 3) неравенство треугольника: $\forall x, y, z \in X \quad \rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

Пара (X, ρ) называется в этом случае *метрическим пространством*. Элементы множества X принято называть *точками* соответствующего пространства. Аксиомы метрики являются естественным обобщением свойств обычного евклидова расстояния на плоскости $\mathbb{R}^2$ и в пространстве $\mathbb{R}^3$. Поэтому функция ρ и в более

общем случае часто называется расстоянием. Аксиома 3 (неравенство треугольника), если говорить неформально, утверждает, что из точки x до точки z нельзя добраться транзитом через точку y быстрее, чем напрямую (длина любой стороны треугольника не превосходит суммы длин двух других сторон). Другими словами, если точка x близка к точке y , а точка y близка к точке z , то точки x и z тоже близки.

Пусть $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_2^n$ — произвольные двоичные наборы длины n . Назовем *расстоянием* между наборами $\tilde{\alpha}$ и $\tilde{\beta}$ число разрядов, которыми они различаются. Обозначим это расстояние $d(\tilde{\alpha}, \tilde{\beta})$:

$$d(\tilde{\alpha}, \tilde{\beta}) = |\{i : \alpha_i \neq \beta_i\}|. \quad (1)$$

Например, расстояние между наборами $\tilde{\alpha} = 01011$ и $\tilde{\beta} = 10010$ равно 3, что можно записать в виде $d(01011, 10010) = 3$, так как у наборов 01011 и 10010 не совпадают первый, второй и пятый разряды. Нетрудно убедиться¹, что

$$d(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^n |\alpha_i - \beta_i|. \quad (2)$$

Равенство (2) можно принять за второе эквивалентное определение расстояния между наборами. Таким образом, нами получена функция $d : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \mapsto \mathbb{Z}$, определенная на всех парах двоичных наборов одинаковой длины и принимающая целые неотрицательные значения. Функция d называется *метрикой Хемминга*, или *расстоянием Хемминга*. Далее везде в тексте за ней сохранено обозначение d . Покажем, что функция d действительно является метрикой.

Задача 1. Доказать, что функция $d(\tilde{\alpha}, \tilde{\beta})$ — метрика на булевом кубе $\mathbb{Z}_2^n$.

Доказательство. Необходимо проверить выполнение всех трех аксиом метрики. Очевидно, что свойства симметричности и неотрицательности функции d следуют из формулы (1). Для доказательства неравенства треугольника используем равенство (2).

¹ Действительно, величина $|\alpha_i - \beta_i|$ равна нулю, когда разряды α_i и β_i совпадают, и равна единице, когда $\alpha_i \neq \beta_i$, в силу того, что $\alpha_i, \beta_i \in \mathbb{Z}_2$.

Пусть $\tilde{\alpha}, \tilde{\beta}, \tilde{\gamma} \in \mathbb{Z}_2^n$ — произвольные наборы. Тогда, согласно свойству модуля $|x + y| \leq |x| + |y|$, получим

$$\begin{aligned} d(\tilde{\alpha}, \tilde{\gamma}) &= \sum_{i=1}^n |\alpha_i - \gamma_i| = \sum_{i=1}^n |(\alpha_i - \beta_i) + (\beta_i - \gamma_i)| \leq \\ &\leq \sum_{i=1}^n |\alpha_i - \beta_i| + \sum_{i=1}^n |\beta_i - \gamma_i| = d(\tilde{\alpha}, \tilde{\beta}) + d(\tilde{\beta}, \tilde{\gamma}). \end{aligned}$$

Утверждение доказано. $\square$

Можно доказать неравенство треугольника $\forall \tilde{\alpha}, \tilde{\beta}, \tilde{\gamma}: d(\tilde{\alpha}, \tilde{\gamma}) \leq d(\tilde{\alpha}, \tilde{\beta}) + d(\tilde{\beta}, \tilde{\gamma})$ и непосредственно по формуле (1). Действительно, если $\alpha_i = \beta_i$ и $\beta_i = \gamma_i$, то $\alpha_i = \gamma_i$. Значит, наборы $\tilde{\alpha}$ и $\tilde{\gamma}$ содержат несовпадающие символы только в тех разрядах, где символы не совпадают либо у $\tilde{\alpha}$ и $\tilde{\beta}$, либо у $\tilde{\beta}$ и $\tilde{\gamma}$. Следовательно, общее количество несовпадающих символов у наборов $\tilde{\alpha}$ и $\tilde{\gamma}$ не превосходит суммарного числа несовпадающих символов у наборов $\tilde{\alpha}$ и $\tilde{\beta}$ и $\tilde{\beta}$ и $\tilde{\gamma}$. Но именно эти числа и были обозначены $d(\tilde{\alpha}, \tilde{\gamma})$, $d(\tilde{\alpha}, \tilde{\beta})$ и $d(\tilde{\beta}, \tilde{\gamma})$.

Таким образом, булев куб с расстоянием Хемминга — метрическое пространство. Если $d(\tilde{\alpha}, \tilde{\beta}) = 1$ (наборы $\tilde{\alpha}, \tilde{\beta}$ различаются ровно одним разрядом), то наборы $\tilde{\alpha}$ и $\tilde{\beta}$ называются *соседними*. Пара соседних наборов называется *ребром* булева куба. Если два набора различаются во всех разрядах, то они называются *противоположными*.

Задача 2. Найти число наборов в кубе $\mathbb{Z}_2^n$: а) соседних с набором $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$; б) противоположных набору $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$.

Решение. Очевидно, что противоположный набору $\tilde{\alpha}$ набор определяется однозначно: надо изменить каждый из его разрядов α_i на противоположный (инвертировать).

Поскольку во множестве $\mathbb{Z}_2$ всего два элемента, то это можно сделать всего одним способом. Соседние же наборы можно получить n различными способами: достаточно выбрать один из n разрядов, инвертировать его, а остальные оставить без изменения. Например, все соседние с $\tilde{\alpha} = 1001$ наборы выглядят так: