

Основные алгоритмы. Домашняя работа 9 неделя

Зайнуллин Амир

1 мая 2023 г.

Задача №1

Чтобы проверить, что (X, \emptyset) является матроидом, докажем что все аксиомы выполняются. $\emptyset \subseteq 2^X$

1. $\emptyset \in \emptyset$, первая аксиома выполняется.
2. Подмножество пустого множества принадлежит пустому множеству, значит вторая аксиома тоже выполняется.
3. если $A, B \in I$, $|B| > |A|$, но такого B не существует. Значит третья аксиома тоже выполняется.

Задача №2

Чтобы проверить, что $(X, 2^X)$ является матроидом, докажем что все аксиомы выполняются. $2^X \subseteq 2^X$.

1. $\emptyset \in 2^X$, первая аксиома выполняется.
2. Любое подмножество 2^X принадлежит 2^X , значит вторая аксиома тоже выполняется.
3. если $A, B \in I$, $|B| > |A|$, то $\exists x \in B \setminus A: A \cup x \in I$. Это верно, потому что I это множество всех подмножеств.

Задача №3

Чтобы проверить, что пара (X, I) , где I - множество подмножеств мощности не больше k , является матроидом, докажем что все аксиомы выполняются. $I \subseteq 2^X$

1. $\emptyset \in I$, первая аксиома выполняется.
2. Любое подмножество множества мощности не больше k принадлежит I , вторая аксиома тоже выполняется.
3. если $A, B \in I$, $|B| > |A|$, то $\exists x \in B \setminus A: A \cup x \in I$. Максимальная мощность B равна k , Тогда максимальная мощность A равна $k - 1$. Тогда $A \cup x \in I$, т.к мощность $A \cup x$ не может быть больше k , и значит оно принадлежит I .

(a) Над полем вычетов по модулю 5:

Для нахождения НОД можно воспользоваться алгоритмом Евклида для многочленов. Для этого нужно последовательно делить больший многочлен на меньший до тех пор, пока не получится многочлен степени меньше, чем делитель. Затем делитель заменяется на остаток от деления и процедура повторяется до тех пор, пока не будет получен многочлен степени 0 (константа). НОД будет равен последнему ненулевому остатку.

Выполним деление многочленов:

$$6x^3 + 2x^2 + x + 2 : x^2 + 4x + 3 = 6x + 22 \text{ (остаток)}$$

$$x^2 + 4x + 3 : 6x + 22 = -x - 1 \text{ (остаток)}$$

$$6x + 22 : -x - 1 = -6 \text{ (остаток)}$$

Последний ненулевой остаток равен $-6x + 30$. Значит, НОД равен $-6x + 30$.

Для нахождения коэффициентов, с которыми нужно сложить данные многочлены для его получения, можно воспользоваться расширенным алгоритмом Евклида для многочленов. Этот алгоритм позволяет находить коэффициенты a и b такие, что НОД равен $af + bg$, где f и g - исходные многочлены.

Выполним расширенный алгоритм Евклида:

$$6x^3 + 2x^2 + x + 2 = (-x - 1)(x^2 + 4x + 3) + (-6x + 5)$$

$$x^2 + 4x + 3 = (-2x - 1)(-6x + 5) + (7x + 8)$$

Последняя строка означает, что НОД равен $7x + 8$. Значит, для получения этого многочлена нужно сложить исходные многочлены с коэффициентами -1 и -2 соответственно:

$$(6x^3 + 2x^2 + x + 2) + (-1)(x^2 + 4x + 3) + (-2)(-6x + 5) = 7x + 8$$

Ответ: НОД равен $-6x + 30$, коэффициенты для получения НОД равны -1 и -2 .

(b) Над полем вычетов по модулю 7:

Выполним деление многочленов:

$$6x^3 + 2x^2 + x + 2 : x^2 + 4x + 3 = 6x + 5 \text{ (остаток)}$$

$$x^2 + 4x + 3 : 6x + 5 = -2x - 2 \text{ (остаток)}$$

$$6x + 5 : -2x - 2 = 1 \text{ (остаток)}$$

Последний ненулевой остаток равен 1. Значит, НОД равен 1.

Выполним расширенный алгоритм Евклида:

$$6x^3 + 2x^2 + x + 2 = (-2x - 2)(x^2 + 4x + 3) + (14x + 8)$$

$$x^2 + 4x + 3 = (-3x + 3)(14x + 8) + (45)$$

Последняя строка означает, что НОД равен 1. Значит, для получения этого многочлена нужно сложить исходные многочлены с коэффициентами -2 и 3 соответственно:

$$(6x^3 + 2x^2 + x + 2) + (-2)(x^2 + 4x + 3) + 3(14x + 8) = 1$$

Ответ: НОД равен 1, коэффициенты для получения НОД равны -2 и 3 .

Заметим, что $x^2 + x - 5 = (x - 2)(x + 3)$, поэтому поле $Z7[x]/(x^2 + x - 5)$ не является полем, так как содержит делители нуля. Чтобы найти нильпотентные элементы, нужно искать элементы, возведение которых в некоторую степень дает ноль. Пусть $f(x)$ — нильпотентный элемент. Тогда найдется такое натуральное число n , что $f(x)^n = 0$ в $Z7[x]/(x^2 + x - 5)$. Это означает, что многочлен $f(x)$ делится на $(x^2 + x - 5)^n$. Но $(x^2 + x - 5)$ и $(x^2 + x - 5)^2$ не имеют общих множителей, поэтому $f(x)$ должен делиться на $(x^2 + x - 5)$, но не на $(x^2 + x - 5)^2$. Таким образом, нильпотентные элементы в $Z7[x]/(x^2 + x - 5)$ — это ровно те многочлены $f(x)$, которые делятся на $(x^2 + x - 5)$, но не делятся на $(x^2 + x - 5)^2$. Такие многочлены имеют вид $f(x) = a(x - b)$, где a и b — элементы поля $Z7$, причем b является корнем многочлена $x^2 + x - 5$ в этом поле. Найдем корни этого многочлена:

$$x^2 + x - 5 \equiv (x + 4)(x - 1) \pmod{7}.$$

Таким образом, корни многочлена $x^2 + x - 5$ в поле $Z7$ — это 1 и 3. Проверяем каждый из них: - Если $b = 1$, то $f(x) = a(x - 1)$, и $f(x)^2 = a^2(x - 1)^2$. Многочлен $x^2 + x - 5$ делит $f(x)$ тогда и только тогда, когда $a(1 - 1) = 0$, то есть $a = 0$. Значит, нильпотентным элементом является только многочлен $f(x) = 0$. - Если $b = 3$, то $f(x) = a(x - 3)$, и $f(x)^2 = a^2(x - 3)^2$. Многочлен $x^2 + x - 5$ делит $f(x)$ тогда и только тогда, когда $(x - 3)$ делит $f(x)$. Значит, a может быть любым элементом поля $Z7$, кроме нуля. Таким образом, нильпотентными элементами являются многочлены вида $f(x) = a(x - 3)$, где a — любой ненулевой элемент поля $Z7$.