О специализации математических формул и утверждений

Андрей П. Немытых
Институт программных систем РАН
г. Переславль-Залесский

Совместное рабочее совещание ИПС РАН и МГТУ имени Н.Э. Баумана
по функциональному языку программирования Рефал

17 июня 2023 г., Москва

Неформальный смысл

Любые вычислений являются символьными:

- Даже когда мы вычисляем приближенное значение в точке интересующей нас функции.
  - Мы заранее договариваемся о том, что считать погрешностью этого вычисления.
  - И саму погрешность тоже вычисляем символьно.
- Обычно, под символьными вычислениями имеют в виду в том или ином смысле автоматизированные вычисления.
  - Например, когда используют некоторый навык и лист бумаги — в качестве дисковой памяти.

Автоматизированные символьные вычисления

Примеры:

- Компьютерная алгебра.
- Оптимизация программ. Преобразование программ.
  - Один из методов: «Специализация программ».

Специализация программ по контексту использования

В простейшем случае пробует решать задачу:

Дано определение (программа) частичной функции
$\mathbf{f(x, y) : N \times M \rightharpoonup D}$ и $\mathbf{x_0 \in N}$
Требуется построить определение $\mathbf{f_{x_0}(y)}$ частичной подфункции
$\mathbf{f(x_0, y) : M \rightharpoonup D}$ такое, что для всех $\mathbf{y \in M}$

$$\text{time}([\![f_{x_0}(y)]\!]) \leq \text{time}([\![f(x_0, y)]\!])$$

- Здесь в знаке $\leq$ – спекуляция. Задача тривиальная.
- Если изменить условие на:
  - для всех $\mathbf{y \in M}$ $\text{time}([\![f_{x_0}(y)]\!]) < \text{time}([\![f(x_0, y)]\!])$
- тогда, в общем случае, задача является алгоритмически неразрешимой.

Специализация

- Любое упражнение по математике для студентов является задачей по специализации некоторой теоремы (утверждения).
- Специализация теоремы (следствие) не всегда является упрощением формулировки этой теоремы — по контексту её использования.

Пример

Пусть π есть длина окружности, диаметр которой равен **1**.

Теорема

$$\pi/4 = \mathbf{1} - \mathbf{1/3} + \mathbf{1/5} - \mathbf{1/7} + \ldots$$

Следствие

$\pi = 3{,}14159265358979323846264338327950288419716939937510$
$582097494459230781640628620899862803482534211706798214$
$808651328230664709384460955058223172535940812848111745 0$
$284102701938521105559644622948954930381964428810975665 9$
$334461284756482337867831652712019091456485669234603486 1$
$045432664821339360726024914127372458700660631558817488 1$
$520920962829254091715364367892590360011330530548820466 5$
$213841469519415116094330572703657595919530921861173819 3$
$261179310511854807446237996274956735188575272489122793 8$
$183011949129833673362440656643086021394946395224737190 7$
$021798609437027705392171762931767523846748184676694051 3$
$200056812714526356082778577134275778960917363717872146 8$
$440901224953430146549585371050792279689258923542019956 1$
$121290219608640344181598136297747713099605187072113499 9$
$999837297804995105973173281609631859502445945534690830 2$
$642522308253344685035261931188171010003137838752886587 5$
$33208381420617177669147303598253490428755468731159 5\ldots$

- Условие студенческой задачи должно быть поставлено на языке, которым владеет студент, — понимать который его уже научили.
- Для компьютера задачу на специализацию можно ставить только на том языке программирования, которому ранее уже обучили этот компьютер.
- Более простое и информативное описание условия задачи даёт больше возможностей для успешного решения задачи.

Пусть дан специализатор Spec программ, написанных на языке программирования $\mathcal{L}$. Можно поставить задачу на специализацию так, что Spec будет пытаться:

- компилировать программы на языке $\mathcal{M}$ в язык $\mathcal{L}$;
  - насколько эффективным получится результат компиляции — это отдельный вопрос.

- верифицировать недетерминированный коммуникационный протокол;

- описывать множества решений некоторых классов уравнений в словах.

Специализации математических формул и утверждений

Рассмотрим

- вариации двух идей А. В. Корлюкова о постановке таких задач на специализацию;
- результаты их решения посредством специализатора SCP4, который по недоразумению называется «суперкомпилятором»;
- задачи на специализацию будут ставиться на языке программирования Рефал.

Понятие критерия делимости

Пусть $\mathbf{N} = \overline{\mathbf{d_n d_{n-1} \dots d_0}}$ - натуральное число, где $\mathbf{d_n > 0}$ и $\mathbf{0 \le d_i \le 9}$, заданное в десятичной системе счисления.

Простейший «критерий делимости» **N** на натуральное число **q**: нужно разделить **N** на **q**, тогда «**N** делится на **q** тогда и только тогда, когда остаток от этого деления равен **0**».

Определение

Критерии делимости определяют факт делимости одного натурального **N** числа на другое **q**, не выполняя соответствующего деления **N** на **q**, в терминах свойств цифр числа **N**. Критерии делимости проще, чем прямое деление **N** на **q**.

Критерий делимости в системе счисл. по основанию 10

Нижеследующее равенство (формулу), являющееся критерием равенства остатков результатов двух сумм при делении их на натуральное число $\mathbf{q}$, обычно принято называть критерием делимости $\mathbb{N} \ni \mathbf{N} = \overline{\mathbf{d_n d_{n-1} \ldots d_0}}$ на $\mathbf{q} \in \mathbb{N}$.

$$(\sum_{\mathbf{k=0}}^{\mathbf{n}} \mathbf{10^k d_k})\%\mathbf{q} = (\sum_{\mathbf{k=0}}^{\mathbf{n}} (\mathbf{10^k}\%\mathbf{q})\mathbf{d_k})\%\mathbf{q}$$

Это равенство верно для всех $\mathbf{N} \in \mathbb{N}$ и параметризовано $\mathbf{q}$. Правая часть этого равенства удовлетворяет требованиям критерия делимости, отмеченным выше.

Критерий делимости в системе счисл. по основанию β

$\mathbb{N} \ni \mathbf{N} = \overline{\mathbf{d_n d_{n-1} \dots d_0}}$ на $\mathbf{q} \in \mathbb{N}$.

Для системы счисления по основанию β критерий будет выглядеть аналогично:

$$(\sum_{\mathbf{k=0}}^{\mathbf{n}} \beta^{\mathbf{k}} \mathbf{d_k}) \% \mathbf{q} = (\sum_{\mathbf{k=0}}^{\mathbf{n}} (\beta^{\mathbf{k}} \% \mathbf{q}) \mathbf{d_k}) \% \mathbf{q}$$

Здесь уже два параметра: β и $\mathbf{q}$.

- $(\sum_{\mathbf{k=0}}^{\mathbf{n}} (\beta^{\mathbf{k}} \% \mathbf{q}) \mathbf{d_k}) \% \mathbf{q}$ суть программа вычисления остатка от деления $\mathbf{N} \in \mathbb{N}$ на $\mathbf{q} \in \mathbb{N}$;
  - эта программа, написанная на языке алгебры, имеет три аргумента (входа): конечную последовательность цифр делимого $\mathbf{N}$, основание системы счисления β и делитель $\mathbf{q}$;

Критерий делимости в системе счисл. по основанию 10

- Следуя А. В. Корлюкову, переведем программу $(\sum_{\mathbf{k=0}}^{\mathbf{n}}(\mathbf{10^k}\%\mathbf{q})\mathbf{d_k})\%\mathbf{q}$ на язык Рефал и будем специализировать её по конкретным значениям параметра $\mathbf{q_0}$.

- Результаты, аналогичные полученным в этих экспериментах, будут получаться и при специализации результата трансляции программы $(\sum_{\mathbf{k=0}}^{\mathbf{n}}(\beta^{\mathbf{k}}\%\mathbf{q})\mathbf{d_k})\%\mathbf{q}$ на язык Рефал по конкретным значениям пары параметров $(\beta_{\mathbf{0}}, \mathbf{q_0})$.

Вариант А. В. Корлюкова:

```
$ENTRY Go { e.ds  = <divide #s.q (e.ds)>; }

divide { s.q (e.ds) = <div  1 0  s.q (e.ds)>; }
```

```
div {
 s.m s.res s.q ( ) = s.res;        /* (∑_{k=0}^{n} 10^k d_k)%q = */
 s.m s.res s.q (e.ds s.d)
        /* ((((10 * (10^{i-1}%q))%q)d_i + ∑_{k=0}^{i-1}(10^k%q)d_k))%q */
                , <* s.m 10>: s.p
                , <% s.p s.q>: s.M
                , <* s.d s.m>: s.D
                , <+ s.res s.D>: s.R
                        = <div s.M s.R s.q (e.ds)>;
}
```

Система переписывания термов:

```
$ENTRY Go { e.ds  = <divide #s.q (e.ds)>; }

divide { s.q (e.ds) = <div  1 0  s.q (e.ds)>; }
```

```
div {
 s.m s.res s.q ( ) = s.res;        /* (∑_{k=0}^{n} 10^k d_k)%q = */
 s.m s.res s.q (e.ds s.d)
        /* ((((10 * (10^{i-1}%q))%q)d_i + ∑_{k=0}^{i-1}(10^k%q)d_k))%q */
     = <div <% <* s.m 10> s.q> <+ s.res <* s.d s.m>> s.q (e.ds)>;
}
```

Система переписывания термов в расширенном синтаксисе Рефала-5:

```
$ENTRY Go { ds_e  = <divide #q_s (ds_e)>; }

divide { q_s (ds_e) = <div  1 0  q_s (ds_e)>; }
```

```
div {
 m_s res_s q_s ( ) = res_s;        /* (∑_{k=0}^{n} 10^k d_k)%q = */
 m_s res_s q_s (ds_e d_s)
        /* ((((10 * (10^{i-1}%q))%q)d_i + ∑_{k=0}^{i-1}(10^k%q)d_k))%q */
     = <div <% <* m_s 10> q_s> <+ res_s <* d_s m_s>> q_s (ds_e)>;
}
```

Вариант А. В. Корлюкова:

```
$ENTRY Go { e.ds  = <divide #s.q (e.ds)>; }

divide { s.q (e.ds) = <div  1 0  s.q (e.ds)>; }
```

```
div {
 s.m s.res s.q ( ) = s.res;      /* (∑_{k=0}^{n} 10^k d_k)%q = */
 s.m s.res s.q (e.ds s.d)
        /* ((((10 * (10^{i-1}%q))%q)d_i + ∑_{k=0}^{i-1}(10^k%q)d_k))%q */
                , <* s.m 10>: s.p
                , <% s.p s.q>: s.M
                , <* s.d s.m>: s.D
                , <+ s.res s.D>: s.R
                        = <div <Const__ s.M> s.R s.q (e.ds)>;
}
Const__ {  e.x = e.x;  }
```

В системе счисления по основанию **10**

```
$ENTRY Go { e.ds  = <divide 3 (e.ds)>; }
.....................................
```

Остаточная программа, построенная суперком. SCP4:

```
$ENTRY Go {
            = 0;
 e.41 s.101 = <F13  (e.41) s.101 >;
}

F13 {                    /* Σ_{k=0}^{n} d_k ⋮ 3 */
 ( ) s.101 = s.101;
 (e.41 s.104) s.101
              , <Add (s.101) s.104 >: s.110
                    = <F13 (e.41) s.110 >;
}
```

В системе счисления по основанию **10**

```
$ENTRY Go { e.ds  = <divide 10 (e.ds)>; }
divide { s.q (e.ds) = <div  1 0  s.q (e.ds)>; }
.....................................................
```

Остаточная программа, построенная суперком. SCP4:

```
$ENTRY Go {                  /* d0 ⋮ 10 */
             = 0;
 e.41 s.101 = s.101;
}
```

В системе счисления по основанию **10**

```
$ENTRY Go { e.ds  = <divide 6 (e.ds)>; }
.....................................
```

Остаточная программа, построенная суперком. SCP4:

```
$ENTRY Go {
            = 0;
 e.41 s.101 = <F13  (e.41) s.101 >;
}

F13 {                    /* 4 × ∑_{k=1}^{n} d_k + d_0 ⋮ 6 */
 ( ) s.101 = s.101;
 (e.41 s.104) s.101
                , <Mul (s.104) 4 >: s.109
                , <Add (s.101) s.109 >: s.112
                       = <F13 (e.41) s.112 >;
}
```

В системе счисления по основанию **10**

```
$ENTRY Go { e.ds  = <divide 37 (e.ds)>; }
.............................................
```

```
$ENTRY Go {.................................}

F13 {              /* ∑_{k=0}^{n/3}(26 × d_{3k+2} + 10 × d_{3k+1} + d_{3k}) ⋮ 37 */
 ( ) s.101 = s.101;
 (e.41 s.104) s.101, <Mul (s.104) 10 >: s.109
                , <Add (s.101) s.109 >: s.112 = <O2 (e.41) s.112 >;  }
O2 {
 ( ) s.112 = s.112;
 (e.41 s.115) s.112, <Mul (s.115) 26 >: s.120
                , <Add (s.112) s.120 >: s.123 = <O1 (e.41) s.123 >;  }
O1 {
 ( ) s.123 = s.123;
 (e.41 s.126) s.123, <Add (s.123) s.126 >: s.132
                   = <F13 (e.41) s.132 >;  }
```

Примеры

Примеры критериев делимости $\overline{\mathbf{d_n d_{n-1} \ldots d_0}}$ на

6: $4 \times \sum_{k=1}^{n} d_k + d_0 \vdots 6$

- $6674 \vdots 6 \Leftrightarrow (4(6+6+7)+4) = 80 \vdots 6 \Leftrightarrow 32 \vdots 6 \Leftrightarrow 14 \vdots 6$
- $2022 \vdots 6 \Leftrightarrow (4(2+2)+2) = 18 \vdots 6 \Leftrightarrow 12 \vdots 6 \Leftrightarrow 6 \vdots 6$

37: $\sum_{k=0}^{n/3}(26 \times d_{3k+2} + 10 \times d_{3k+1} + d_{3k}) \vdots 37$

- $2023 \vdots 37 \Leftrightarrow (2+20+3) = 25 \vdots 37$
- $18446744073709551615 \vdots 37 \Leftrightarrow 1010 \vdots 37 \Leftrightarrow 11 \vdots 37$

12: $4 \times \sum_{k=2}^{n} d_k + 10 \times d_1 + d_0 \vdots 12$

999: $\sum_{k=0}^{n/3}(100 \times d_{3k+2} + 10 \times d_{3k+1} + d_{3k}) \vdots 999$

Основные понятия

Пусть $\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$ и эти множества суть алгебраические поля. Говорят, что поле $\mathbf{F}$ есть подполе поля $\mathbf{K}$, если арифметика в поле $\mathbf{F}$ совпадает с арифм. поля $\mathbf{K}$ (на его подмножестве $\mathbf{F}$). В частности, поле $\mathbf{F}$ замкнуто относительно его арифм. операций.

Определение

Подполе $\mathbf{M} \subsetneq \mathbf{K}$ поля $\mathbf{K}$ называется конечным расширением поля $\mathbf{F}$ в поле $\mathbf{K}$, если $\mathbf{F}$ есть подполе поля $\mathbf{M}$ ($\mathbf{F} \subsetneq \mathbf{M}$) и $\mathbf{M}$ является конечномерным линейным пространством над полем $\mathbf{F}$.

Пусть дано поле $\mathbf{P}$, тогда над $\mathbf{P}$ определено кольцо многочленов от $\mathbf{n}$ переменных $\mathbf{P}[\mathbf{x_1}, \ldots, \mathbf{x_n}]$. Коэффициенты этих многочленов принадлежат полю $\mathbf{P}$.

Алгебраически замкнутыме поля

Определение

Поле $\mathbf{K}$ называется алгебраически замкнутым, если любой многочлен ненулевой степени из $\mathbf{K}[\mathbf{x}]$ имеет хотя бы один корень из $\mathbf{K}$.

Далее будем предполагать, что поле $\mathbf{K}$ является алгебраически замкнутым.

Число $\alpha \in \mathbf{K}$ называется алгебраическим над подполем $\mathbf{F} \subsetneq \mathbf{K}$, если оно является корнем некоторого многочлена из $\mathbf{F}[\mathbf{x}]$.

- $\forall \beta \in \mathbf{F}$, β является алгебраическим над $\mathbf{F}$.

Определение

Если любое $\alpha \in \mathbf{K}$, алгебраическое над $\mathbf{F}$, принадлежит $\mathbf{F}$, тогда поле $\mathbf{F}$ называется алгебраически замкнутым подполем в поле $\mathbf{K}$.

Алгебраически порожденные расширения полей

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$

- Наименьшее подполе $\mathbf{M}$, содержащее подмножество $\mathbf{S} \subsetneq \mathbf{K}$ и $\mathbf{F}$, обозначается $\mathbf{M}(\mathbf{S})$ и называется полем, порождённым множеством $\mathbf{S}$ над полем $\mathbf{F}$.

- Расширения поля, порождённые одним элементом, называются простыми расширениями.

Определение

Расширение $\mathbf{M}$ поля $\mathbf{F}$ называется алгебраически порожденным, если оно порождается конечным множеством алгебраических элементов поля $\mathbf{F}$.

Алгебраически порожденные расширения полей

Пусть характеристика поля $\mathbf{F}$ равна нулю.

Теорема

Любое конечное расширение поля $\mathbf{F}$ является алгебраически порожденным.

Теорема

Любое конечное расширение поля $\mathbf{F}$ можно построить посредством конечной последовательности простых алгебраических расширений.

$$\mathbf{F} = \mathbf{M_0} \subsetneq \mathbf{M_1} \subsetneq \ldots \subsetneq \mathbf{M_{n-1}} \subsetneq \mathbf{M_n} = \mathbf{M}$$

Вопросы

Пусть характеристика поля $\mathbf{F}$ равна нулю.

Теорема

Любое конечное расширение поля $\mathbf{F}$ можно построить посредством конечной последовательности простых алгебраических расширений.

$$\mathbf{F} = \mathbf{M_0} \subsetneq \mathbf{M_1} \subsetneq \ldots \subsetneq \mathbf{M_{n-1}} \subsetneq \mathbf{M_n} = \mathbf{M}$$

- Что значит построить поле - конечное расширение другого поля?
- Зачем нужны конечные расширения полей?

Зачем нужны конечные расширения полей

- Современный подход к теории Галуа заключается в изучении автоморфизмов расширения произвольного поля при помощи группы Галуа, соответствующей данному расширению.
- Эварист Галуа излагал свою теорию в других терминах.

Теория Галуа позволяет решать задачи:

- Какие алгебраические уравнения от одной переменной разрешимы в радикалах?
  - Т.е. их корни можно выразить используя только сложение, вычитание, умножение, деление и извлечение корня.
- Какие геометрические фигуры можно построить циркулем и линейкой?
- Имеет ли функция первообразную, которая выражается через элементарные функции?
  - Например, интеграл $\int \frac{\sin(x)}{x} dx$ не берётся в элементарных функциях.

Зачем нужны конечные расширения полей

- Современный подход к теории Галуа заключается в изучении автоморфизмов расширения произвольного поля при помощи группы Галуа, соответствующей данному расширению.
- Эварист Галуа излагал свою теорию в других терминах.

Построить поле - конечное расширение другого поля

Процедура

построения расширения данного поля, позволяющая добавить в него корень многочлена $\mathbf{p(x)}$, - это взятие факторкольца кольца многочленов над этим полем по главному идеалу, порожденному $\mathbf{p(x)}$.

Простые числа и неприводимые многочлены

Аналогом простого числа в кольце целых чисел является неприводимый многочлен в кольце многочленов.

- Простое число $\mathbf{q}$ не делится на другие целые числа, кроме $-\mathbf{q}$ и $\mathbf{1}$, $-\mathbf{1}$.
- Неприводимый многочлен $\mathbf{p(x)} \in \mathbf{F[x]}$ не делится на другие многочлены из $\mathbf{F[x]}$, кроме $\mathbf{c}$ и $\mathbf{c} \times \mathbf{p(x)}$, где $\mathbf{c} \in \mathbf{F}$ и $\mathbf{c} \neq \mathbf{0}$.

Простые числа и неприводимые многочлены

Аналогом простого числа в кольце целых чисел является неприводимый многочлен в кольце многочленов.

- Факторкольцо $\mathbb{Z}/\mathbf{q}$ кольца целых чисел $\mathbb{Z}$ по простому числу $\mathbf{q}$ является полем.
  - Элементы $\mathbb{Z}/\mathbf{q}$ суть остатки от деления на $\mathbf{q}$.
- Факторкольцо $\mathbf{F}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ кольца $\mathbf{F}[\mathbf{x}]$ по неприводимому многочлену $\mathbf{p}(\mathbf{x})$ является полем.
  - Элементы $\mathbf{F}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ суть остатки от деления на $\mathbf{p}(\mathbf{x})$.

Что значит построить поле - конечное расширение другого поля

Процедура

построения расширения данного поля, позволяющая добавить в него корень многочлена $\mathbf{p(x)}$, - это взятие факторкольца кольца многочленов над этим полем по главному идеалу, порожденному $\mathbf{p(x)}$.

- Факторкольцо $\mathbf{F[x]/p(x)}$ кольца $\mathbf{F[x]}$ по неприводимому многочлену $\mathbf{p(x)}$ является полем.
  - Элементы $\mathbf{F[x]/p(x)}$ суть остатки от деления на $\mathbf{p(x)}$.

Даны поле $\mathbf{F}$ и многочлен $\mathbf{q(x)} \in \mathbf{F[x]}$, неприводимый над $\mathbf{F}$.
Построить арифметику остатков от деления многочленов на $\mathbf{q(x)}$.

Процедура

построения расширения данного поля, позволяющая добавить в него корень многочлена $\mathbf{p(x)}$, - это взятие факторкольца кольца многочленов над этим полем по главному идеалу, порожденному $\mathbf{p(x)}$.

- Факторкольцо $\mathbf{F[x]/p(x)}$ кольца $\mathbf{F[x]}$ по неприводимому многочлену $\mathbf{p(x)}$ является полем.
  - Элементы $\mathbf{F[x]/p(x)}$ суть остатки от деления на $\mathbf{p(x)}$.

Пример

Пусть поле $\mathbf{F}$ не содержит корни уравнения $\mathbf{x^2 + 1 = 0}$.
$\Rightarrow$ Многочлен $\mathbf{x^2 + 1 = 0}$ является неприводимым над полем $\mathbf{F}$.
$\Rightarrow$ факторкольцо $\mathbf{M = F[x]/(x^2 + 1)}$ является полем.
Поле $\mathbf{M}$ содержит корень уравнения $\mathbf{x^2 + 1 = 0}$ — образ многочлена $\mathbf{x}$ при отображении факторизации.

Постановка задачи

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, характеристика поля $\mathbf{F}$ равна нулю.

Теорема

Любое конечное расширение поля $\mathbf{F}$ можно построить посредством конечной последовательности простых алгебраических расширений.

$$\mathbf{F} = \mathbf{M_0} \subsetneq \mathbf{M_1} \subsetneq \ldots \subsetneq \mathbf{M_{n-1}} \subsetneq \mathbf{M_n} = \mathbf{M}$$

- Факторкольцо $\mathbf{F}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ кольца $\mathbf{F}[\mathbf{x}]$ по неприводимому многочлену $\mathbf{p}(\mathbf{x})$ является полем.
  - Элементы $\mathbf{F}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ суть остатки от деления на $\mathbf{p}(\mathbf{x})$.

Даны поля $\mathbf{F}, \mathbf{K}$ и многочлен $\mathbf{q}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}]$ неприводимый над $\mathbf{F}$.
Построить арифметику остатков от деления многочленов на $\mathbf{q}(\mathbf{x})$.

Равномерность конструкции

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, характеристика поля $\mathbf{K}$ равна нулю.

Теорема

Любое конечное расширение поля $\mathbf{F}$ можно построить посредством конечной последовательности простых алгебраических расширений.

$$\mathbf{F} = \mathbf{M_0} \subsetneq \mathbf{M_1} \subsetneq \ldots \subsetneq \mathbf{M_{n-1}} \subsetneq \mathbf{M_n} = \mathbf{M}$$

Процедура

построения расширения данного поля конструктивна и равномерна по множеству подполей $\mathbf{F}$ поля $\mathbf{K}$ характеристики $\mathbf{0}$.

Даны поля $\mathbf{F}, \mathbf{K}$ и многочлен $\mathbf{q(x)} \in \mathbf{F[x]}$ неприводимый над $\mathbf{F}$. Построить арифметику остатков от деления многочленов на $\mathbf{q(x)}$.

Постановка задачи

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, поле $\mathbf{K}$ нулевой характеристики алгебраически замкнуто.

- $\mathbf{F} = \mathbb{Q}$, $\mathbf{K} = \mathbb{C}$

- Факторкольцо $\mathbb{Q}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ кольца $\mathbb{Q}[\mathbf{x}]$ по неприводимому многочлену $\mathbf{p}(\mathbf{x})$ является полем.
  - Элементы $\mathbb{Q}[\mathbf{x}]/\mathbf{p}(\mathbf{x})$ суть остатки от деления на $\mathbf{p}(\mathbf{x})$.

Дан многочлен $\mathbf{q}(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ неприводимый над $\mathbb{Q}$. Построить арифметику остатков от деления многочленов на $\mathbf{q}(\mathbf{x})$.

Постановка задачи №1 на специализацию

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, поле $\mathbf{K}$ нулевой характеристики алгебраически замкнуто.

- $\mathbf{F} = \mathbb{Q}$, $\mathbf{K} = \mathbb{C}$
- Многочлен $\mathbf{q_0(x) = x^2 + 1} \in \mathbb{Q}[\mathbf{x}]$ неприводим над $\mathbb{Q}$.
- Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 + 1})$ кольца $\mathbb{Q}[\mathbf{x}]$ по неприводимому многочлену $\mathbf{x^2 + 1}$ является полем.
  - Элементы $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 + 1})$ суть остатки от деления на $\mathbf{x^2 + 1}$.

Описаны в виде программы на языке Рефал:

- функции арифметики в поле $\mathbb{Q}$;
- для произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$.

Постановка задачи №1 на специализацию

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, поле $\mathbf{K}$ нулевой характеристики алгебраически замкнуто.

- $\mathbf{F} = \mathbb{Q}$, $\mathbf{K} = \mathbb{C}$
- Многочлен $\mathbf{q_0(x) = x^2 + 1} \in \mathbb{Q}[\mathbf{x}]$ неприводим над $\mathbb{Q}$.
- Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 + 1})$ является полем. Элементы $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 + 1})$ суть остатки от деления на $\mathbf{x^2 + 1}$.

Описаны в виде программы `FieldExt.ref` + `Q.ref` на языке Рефал:

`Q.ref`: функции арифметики в поле $\mathbb{Q}$;

`ieldExt.ref`: для произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$.

Функции арифметики в поле $\mathbb{Q}$ объявлены внешними для модуля `FieldExt.ref`.

Постановка задачи №1 на специализацию

Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ является полем. Элементы кольца $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ суть остатки от деления на $\mathbf{x^2+1}$.

Описаны в виде программы `FieldExt.ref` + `Q.ref` на языке Рефал:

`Q.ref`: функции арифметики в поле $\mathbb{Q}$;

`ieldExt.ref`: $\forall$ поля $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения $\forall$ поля $\mathbf{F}$ характеристики $\mathbf{0}$.

Функции ариф. в $\mathbb{Q}$ объявлены внешними для модуля `FieldExt.ref`.

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith #oper_s ((#c_e) (#d_e)) ((#a_e) (#b_e)) ( ⌞√(x^2 + 1)⌟ )>
```

Подзадача №1^{-1} на специализацию

Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ является полем. Элементы кольца $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ суть остатки от деления на $\mathbf{x^2+1}$.

Описаны в виде программы `FieldExt.ref` + `Q.ref` на языке Рефал:

`Q.ref`: функции арифметики в поле $\mathbb{Q}$;

`ieldExt.ref`: $\underline{\forall \text{ поля}}$ $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения $\underline{\forall \text{ поля}}$ $\mathbf{F}$ характеристики $\mathbf{0}$.

Функции ариф. в $\mathbb{Q}$ объявлены внешними для модуля `FieldExt.ref`.

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith Inv ((#be) (#ae)) ( ⌞√(x^2 + 1)⌟ )>
```

Деление в кольце $\mathbf{F[x]}$ по модулю неприводимого $\mathbf{q(x)}$

$$\mathbf{p_1(x), p_2(x), q(x) \in F[x], p_2(x) \neq 0}$$

$$\mathbf{p_1(x)/p_2(x)} \mod (\mathbf{q(x)}) = \mathbf{p_1(x)} \times (\mathbf{1/p_2(x)}) \mod (\mathbf{q(x)})$$

Деление в кольце $\mathbf{F}[\mathbf{x}]$ по модулю неприводимого $\mathbf{q}(\mathbf{x})$

$$\mathbf{p_1}(\mathbf{x}), \mathbf{p_2}(\mathbf{x}), \mathbf{q}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}], \mathbf{p_2}(\mathbf{x}) \neq \mathbf{0}$$

$$\mathbf{p_1}(\mathbf{x})/\mathbf{p_2}(\mathbf{x}) \mod (\mathbf{q}(\mathbf{x})) = \mathbf{p_1}(\mathbf{x}) \times (\mathbf{1}/\mathbf{p_2}(\mathbf{x})) \mod (\mathbf{q}(\mathbf{x}))$$

Теорема (алгоритм) Евклида

$\forall \mathbf{u}(\mathbf{x}), \mathbf{v}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}]$, где $\mathbf{u}(\mathbf{x}) \neq \mathbf{0}, \mathbf{v}(\mathbf{x}) \neq \mathbf{0}$, существуют $\mathbf{g}(\mathbf{x}), \mathbf{h}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}]$ такие, что

$$\mathbf{u}(\mathbf{x}) \times \mathbf{g}(\mathbf{x}) + \mathbf{v}(\mathbf{x}) \times \mathbf{h}(\mathbf{x}) = \gcd(\mathbf{u}(\mathbf{x}), \mathbf{v}(\mathbf{x}))$$

$$\Downarrow$$

$$\exists\, \mathbf{g}(\mathbf{x}), \mathbf{h}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}].\ \mathbf{p_2}(\mathbf{x}) \times \mathbf{g}(\mathbf{x}) + \mathbf{q}(\mathbf{x}) \times \mathbf{h}(\mathbf{x}) = \gcd(\mathbf{p_2}(\mathbf{x}), \mathbf{q}(\mathbf{x}))$$

$\mathbf{q}(\mathbf{x})$ неприводимый, следовательно, $\gcd(\mathbf{p_2}(\mathbf{x}), \mathbf{q}(\mathbf{x})) = \mathbf{1}$.

Имеем: $\mathbf{p_2}(\mathbf{x}) \times \mathbf{g}(\mathbf{x}) + \mathbf{q}(\mathbf{x}) \times \mathbf{h}(\mathbf{x}) = \mathbf{1}$.

Следовательно, $(\mathbf{p_2}(\mathbf{x}) \times \mathbf{g}(\mathbf{x})) \mod (\mathbf{q}(\mathbf{x})) = \mathbf{1}$.

Откуда: $(\mathbf{p_2^{-1}}(\mathbf{x}) = \mathbf{g}(\mathbf{x})) \mod (\mathbf{q}(\mathbf{x}))$.

Подзадача №1^{-1} на специализацию

Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ является полем. Элементы кольца $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2+1})$ суть остатки от деления на $\mathbf{x^2+1}$.

Описаны в виде программы `FieldExt.ref` + `Q.ref` на языке Рефал:

`Q.ref`: функции арифметики в поле $\mathbb{Q}$;

`ieldExt.ref`: $\underline{\forall \text{ поля}}$ $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения $\underline{\forall \text{ поля}}$ $\mathbf{F}$ характеристики $\mathbf{0}$.

Функции ариф. в $\mathbb{Q}$ объявлены внешними для модуля `FieldExt.ref`.

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith Inv ((#be) (#ae)) ( ⌞√(x^2 + 1)⌟ )>
```

Подзадача №1^{-1} на специализацию

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith Inv ((#be) (#ae)) ( ⌊√(x^2 + 1)⌋ )>
```

Результат специализации суперкомпилятором SCP4

```
$ENTRY formulai {
  (be) ae = ⌈⌊(−be/(be^2+ae^2))x + (ae/(be^2+ae^2))⌋⌉ ;
}
```

- Грубая схема - кодировка.
- a_e,$b_e \in \mathbb{Q}$.
- Первое приближение.

Подзадача №1^{-1} на специализацию

Функции ариф. в $\mathbb{Q}$ объявлены внешними для модуля `FieldExt.ref`.
Их определения и свойства недоступны для SCP4.

Начальная конфигурация из модуля `FieldExt.ref`:

```
$EXTERN Q_Div, Q_Mul, Q_Sub, Q_Add;
        <F_Arith Inv ((#be) (#ae)) ( ⌊√(x^2 + 1)⌋ )>
```

Результат специализации суперкомпилятором SCP4

```
$ENTRY formulai {
(be) ae = ⌈⌊(−1/be)/(1−ae(0 − (ae/be))/be)x +
          (0 − (0 + 1 × ((0 − (ae/be))/be)))/(1−ae(0 − (ae/be))/be)⌋⌉ ;
}
```

- Кодировка.
- a_e,$b_e \in \mathbb{Q}$; `Q_Div` $= /$, `Q_Mul` $= \times$, `Q_Sub` $= -$, `Q_Add` $= +$;
- Приближение.

Подзадача №1^{-1} на специализацию

Остаточная программа:

```
$EXTERN Q_Div, Q_Mul, Q_Sub, Q_Add;

* p(x) = ((b) (a)) = b*x+a – многочлен; требуется вычислить 1/p(x)
$ENTRY formulai { (be) ae = <C1 (be) (ae) <Q_Div (1) be>>; }

C1 { (e.1) (e.2) e.x1 =                    /* 0-(a/b) = -a/b */
        <C2 (e.1) (e.2) (e.x1) <Q_Sub (0) <Q_Mul (e.2) e.x1>>>; }
.....................................................
* e.x4 = (0-(a/b))/b = -a/b^2;      e.x6 = 1 - a(0-(a/b))/b = 1 - (-a^2/b^2),
* e.y3 = (-1/b)/(1 - a(0-(a/b))/b) = -b/(b^2 + a^2)
C6 { (e.x4) (e.x6) e.y3 =     /* e.y4 = 0-(0+1*((0-(a/b))/b)) = a/b^2 */
     <C7 (e.x6) (e.y3) <Q_Sub (0) <Q_Add (0) <Q_Mul (1) e.x4>>>>>;
}
C7 {              /* (0-(0+1*((0-(a/b))/b)))/(1 - a(0-(a/b))/b)
                     = (a/b^2)/(1 + a^2/b^2) = a/(b^2 + a^2) */
(e.x6) (e.y3) e.y4 , <Q_Div (e.y4) e.x6>: e.y7 = (e.y3) (e.y7); }
* 1/p(x) = (-1/b)/(1-a(0-(a/b))/b)_ _(0-(0+1*((0-(a/b))/b)))/(1-a(0-(a/b))/b)
```

Подзадача №1^{-1} на специализацию

Остаточная программа:

```
$EXTERN Q_Div, Q_Mul, Q_Sub, Q_Add;

* p(x) = ((b) (a)) = b*x+a – многочлен; требуется вычислить 1/p(x)
$ENTRY formulai { (be) ae = <C1 (be) (ae) <Q_Div (1) be>>; }

C1 { (e.1) (e.2) e.x1 =                    /* 0-(a/b) = -a/b */
        <C2 (e.1) (e.2) (e.x1) <Q_Sub (0) <Q_Mul (e.2) e.x1>>>; }
.....................................................
* e.x4 = (0-(a/b))/b = -a/b^2;      e.x6 = 1 - a(0-(a/b))/b = 1 - (-a^2/b^2),
* e.y3 = (-1/b)/(1 - a(0-(a/b))/b) = -b/(b^2 + a^2)
C6 { (e.x4) (e.x6) e.y3 =     /* e.y4 = 0-(0+1*((0-(a/b))/b)) = a/b^2 */
     <C7 (e.x6) (e.y3) <Q_Sub (0) <Q_Add (0) <Q_Mul (1) e.x4>>>>>;
}
C7 {              /* (0-(0+1*((0-(a/b))/b)))/(1 - a(0-(a/b))/b)
                     = (a/b^2)/(1 + a^2/b^2) = a/(b^2 + a^2) */
(e.x6) (e.y3) e.y4 , <Q_Div (e.y4) e.x6>: e.y7 = (e.y3) (e.y7); }
* 1/p(x) = (-1/b)/(1-a(0-(a/b))/b)_ _(0-(0+1*((0-(a/b))/b)))/(1-a(0-(a/b))/b)
```

Постановка задачи №2 на специализацию

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, характеристика поля $\mathbf{F}$ равна нулю.

- $\mathbf{F} = \mathbb{Q}$, $\mathbf{K} = \mathbb{C}$
- Многочлен $\mathbf{q_0(x) = x^2 - 2} \in \mathbb{Q}[\mathbf{x}]$ неприводим над $\mathbb{Q}$.
- Факторкольцо $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 - 2})$ кольца $\mathbb{Q}[\mathbf{x}]$ по неприводимому многочлену $\mathbf{x^2 - 2}$ является полем.
  - Элементы $\mathbb{Q}[\mathbf{x}]/(\mathbf{x^2 - 2})$ суть остатки от деления на $\mathbf{x^2 - 2}$.

Описаны в виде программы на языке Рефал:

- функции арифметики в поле $\mathbb{Q}$;
- для произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$ конструкции кольца $\mathbf{F}[\mathbf{x}]$ и простого расширения произвольного поля $\mathbf{F}$ характеристики $\mathbf{0}$.

Подзадача №2× на специализацию

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith Mul ((#ce) (#de)) ((#ae) (#be)) ( ⌊x^2 − 2⌋ )>
```

Результат специализации суперкомпилятором SCP4

```
$ENTRY formula2m {
  (ce) (de) (ae) be = ⌈⌊(deae+cebe)x + (debe+2ceae)⌋⌉ ;
}
```

- Грубая схема - кодировка.
- $a_e, b_e, c_e, d_e \in \mathbb{Q}$.
- Первое приближение.

Подзадача №2× на специализацию

Начальная конфигурация из модуля `FieldExt.ref`:

```
<F_Arith Mul ((#ce) (#de)) ((#ae) (#be)) ( ⌞x^2 − 2⌟ )>
```

Результат специализации суперкомпилятором SCP4

```
$ENTRY formula2m {
 (ce)(de)(ae) be = ⌜⌞((deae+cebe)−0×(ceae))x+(debe−(−2((ceae)/1)))⌟⌝;
}
```

- Кодировка.
- $a_e, b_e, c_e, d_e \in \mathbb{Q}$;
  Q_Div $= /$, Q_Mul $= \times$, Q_Sub $= -$, Q_Add $= +$;
- Приближение.

Подзадача №2× на специализацию

Остаточная программа:

```
$EXTERN Q_Div, Q_Mul, Q_Sub, Q_Add;
/* p(x) = ((c) (d)) = c*x+d, q(x) = ((a) (b)) = a*x+b – многочлены;
   требуется вычислить p(x)q(x) */
$ENTRY formula2m1 {                                   /* e.y3 = c*a */
 (ce) (de) (ae) be = <C1 (ce) (de) (ae) (be) <Q_Mul (ce) ae>>; }

C1  { (e.2) (e.3) (e.4) (e.5) e.y3 =                  /* e.y6 = d*a */
            <C2 (e.2) (e.3) (e.5) (e.y3) <Q_Mul (e.3) e.4>>; }
.....................................................
* e.y9 =(c*a)/1 = c*a;   e.y8 = d*b, e.y7 = d*a + c*b
C5  { (e.y7) (e.y8) e.y9 =        /* e.z6 = (d*a + c*b) - 0*(c*a) */
        <C6 (e.y8) (e.y9) <Q_Sub (e.y7) <Q_Mul (0) e.y9>>>>; }
C6  { (e.y8) (e.y9) e.z6   /* (d*b) -(-2*((c*a)/1)) = d*b + 2*c*a */
        , <Q_Sub (e.y8) <Q_Mul ('-'2) e.y9>>: e.z7 = (e.z6) (e.z7); }
/* p(x)q(x) = _(((d*a + c*b)-0*(c*a))_ _(d*b-(-2*((c*a)/1))))_
            = ((d*a + c*b) (d*b + 2*c*a)) */
```

Постановка задачи

$\mathbf{F} \subsetneq \mathbf{M} \subsetneq \mathbf{K}$, характеристика поля $\mathbf{F} = \mathbf{p}, \mathbf{p} \neq \mathbf{0}$.

- Следовательно, $\mathbf{p}$ простое. Все теоремы остаются верными. Теоретические конструкции технически усложняются.

Любое конечное поле изоморфно полю Галуа $\mathbb{F}_{\mathbf{p^n}}$, состоящему из $\mathbf{p^n}$ элементов, где $\mathbf{p}$ простое. Для любых $\mathbf{p}, \mathbf{n} \in \mathbb{N}$, где $\mathbf{p}$ простое, существует поле Галуа $\mathbb{F}_{\mathbf{p^n}}$. Характеристика поля $\mathbb{F}_{\mathbf{p^n}}$ равна $\mathbf{p}$.

Постановка задачи

$\mathbf{F} = \mathbb{F}_{\mathbf{p^n}}, \mathbf{K} = \mathbb{Z}_{\mathbf{p}}(\mathbf{x})$

- Где $\mathbb{Z}_{\mathbf{p}}(\mathbf{x})$ есть поле рациональных функций с коэффициентами по модулю $\mathbf{p}$. Элементы $\mathbb{Z}_{\mathbf{p}}(\mathbf{x})$ суть выражения вида $\mathbf{r(x)/q(x)}$; $\mathbf{r(x)}, \mathbf{q(x)} \in \mathbb{Z}_{\mathbf{p}}[\mathbf{x}], \mathbf{q(x)} \not\equiv \mathbf{0}$.

А. В. Корлюков проводил эксперименты с SCP4. См. каталог demo в дистрибутиве SCP4.