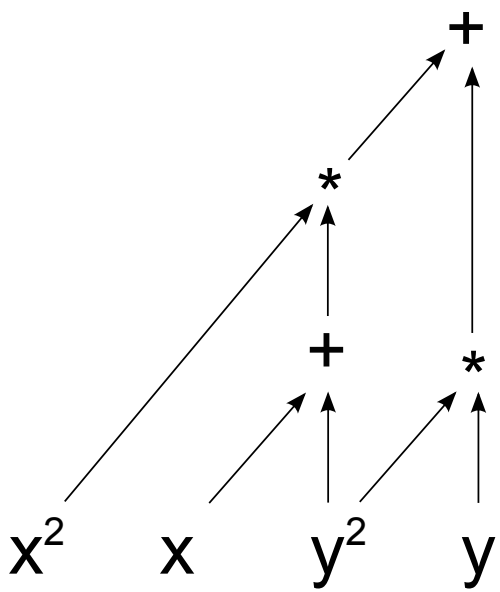
Схемы вычисления полиномов и их приложения

Михаил Кожевников

17 июня 2010 г.

Схемы вычисления полиномов

$$x^3 + x^2y^2 + y^3$$



$$\alpha_1 = x$$
$$\alpha_2 = x^2$$
$$\alpha_3 = y$$
$$\alpha_4 = y^2$$
$$\beta_1 = \alpha_3 \cdot \alpha_4 = y^3$$
$$\beta_2 = \alpha_1 + \alpha_4 = x + y^2$$
$$\beta_3 = \beta_2 \cdot \alpha_2 = x^3 + x^2y^2$$
$$\beta_4 = \beta_3 + \beta_1 = x^3 + x^2y^2 + y^3$$

Приложения

- Символьно-численные интерфейсы

Приложения

- Символьно-численные интерфейсы
- Метод редукции на основе СВП

Цели работы

- Сравнение методов построения СВП

Цели работы

- Сравнение методов построения СВП
- Реализация метода редукции на основе СВП (РСВП)

Цели работы

- Сравнение методов построения СВП
- Реализация метода редукции на основе СВП (РСВП)
- Оценка эффективности РСВП

Цели работы

- Сравнение методов построения СВП
- Реализация метода редукции на основе СВП (РСВП)
- Оценка эффективности РСВП
- Рассмотрение возможных улучшений РСВП

Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов

Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов
- Применяется для
  - проверки принадлежности идеалу

Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов
- Применяется для
  - проверки принадлежности идеалу
  - построения базиса Грёбнера
  - ...

Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов
- Применяется для
  - проверки принадлежности идеалу
  - построения базиса Грёбнера
  - ...
- Простейший алгоритм – последовательное исключение старшего монома

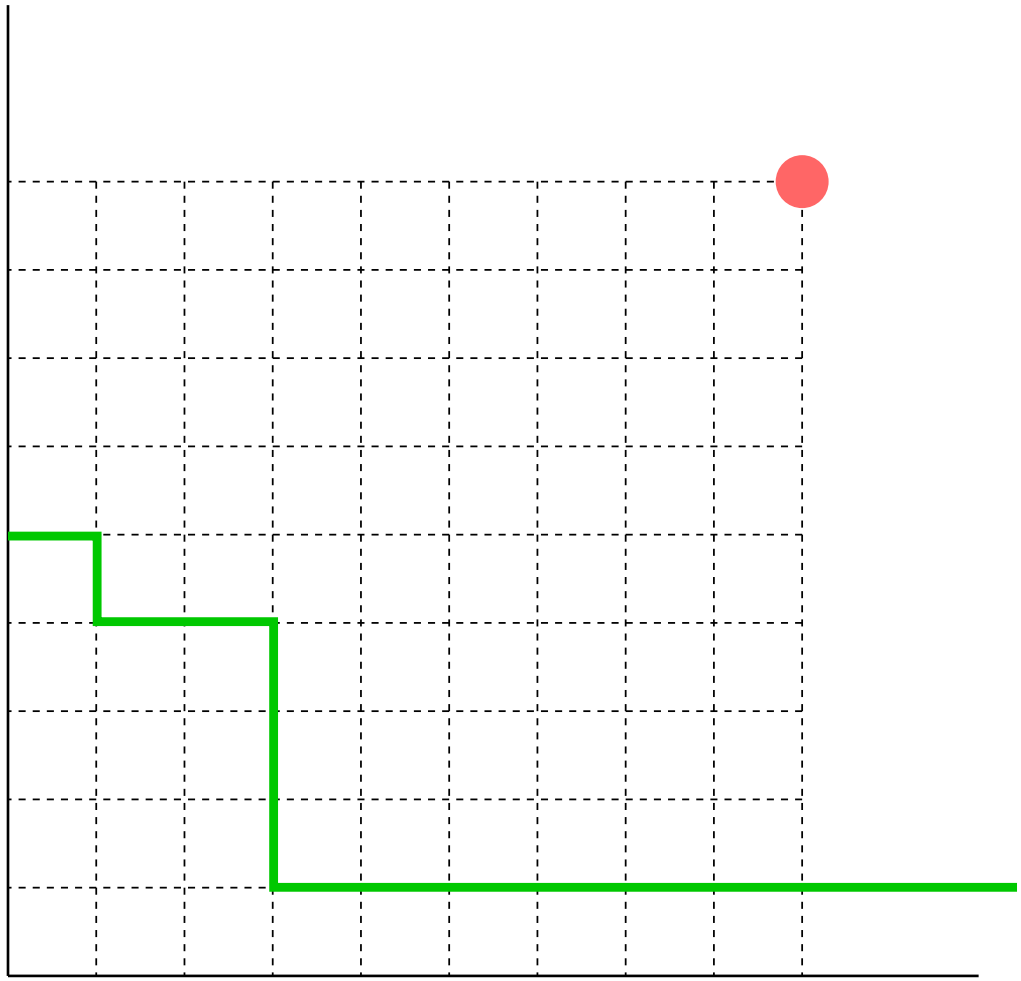
Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов
- Применяется для
  - проверки принадлежности идеалу
  - построения базиса Грёбнера
  - ...
- Простейший алгоритм – последовательное исключение старшего монома
- Сложность существенно зависит от входных данных

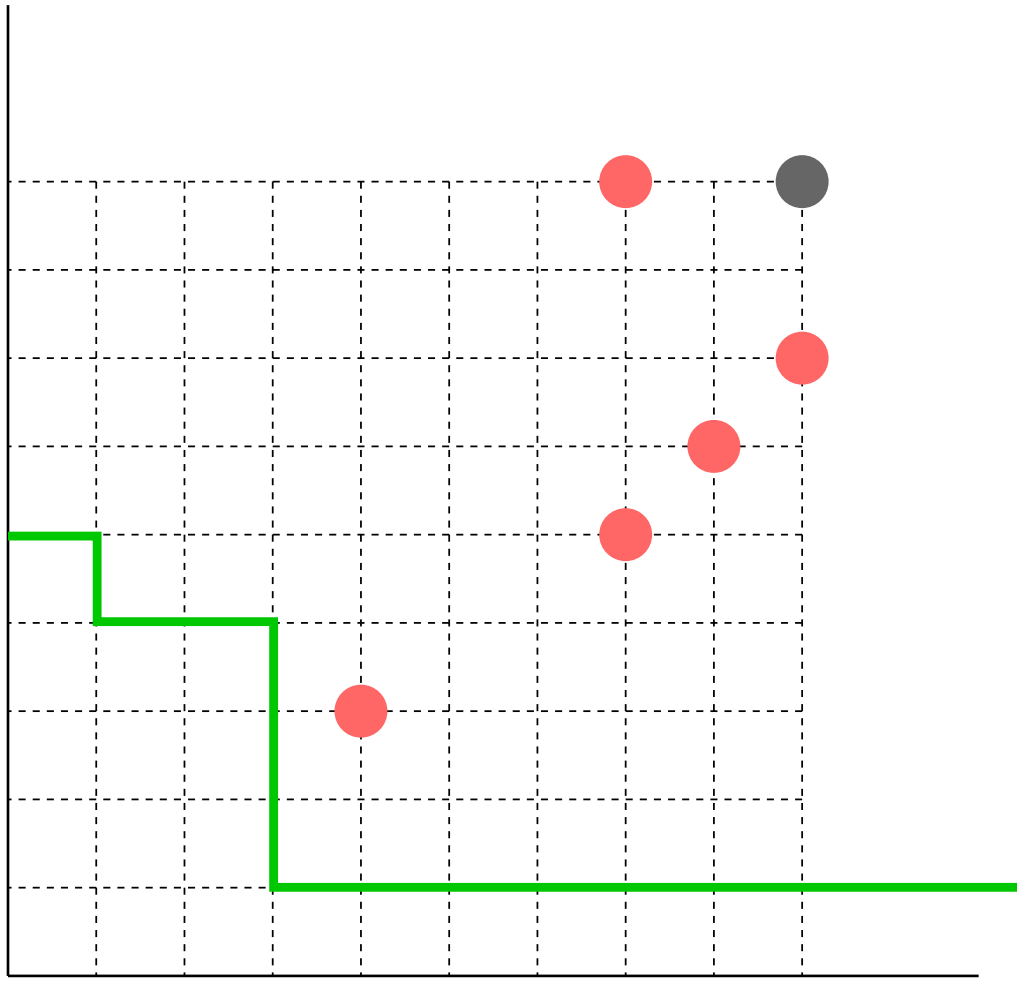
Задача редукции полинома

- Редукция – это поиск остатка от деления полинома на набор полиномов
- Применяется для
  - проверки принадлежности идеалу
  - построения базиса Грёбнера
  - ...
- Простейший алгоритм – последовательное исключение старшего монома
- Сложность существенно зависит от входных данных
- Количество членов в полиноме может интенсивно расти

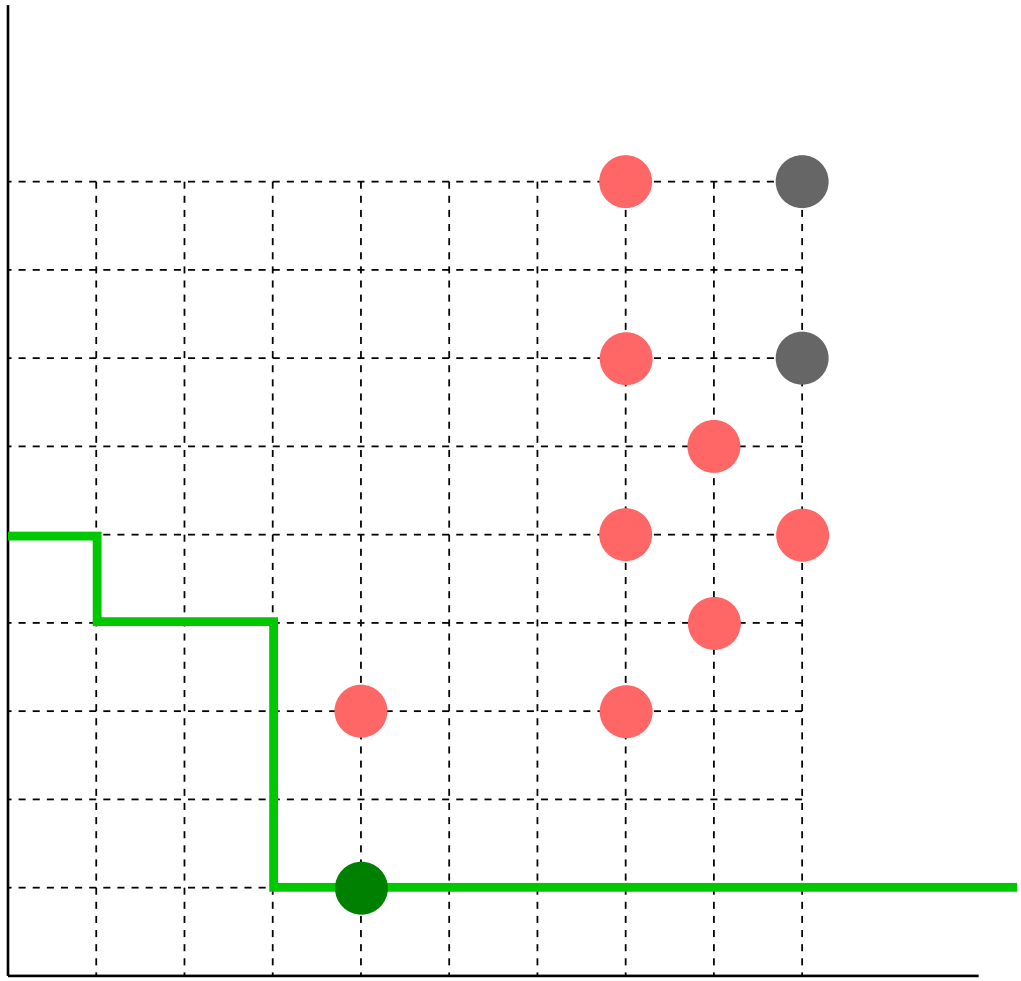
Обычный алгоритм редукции



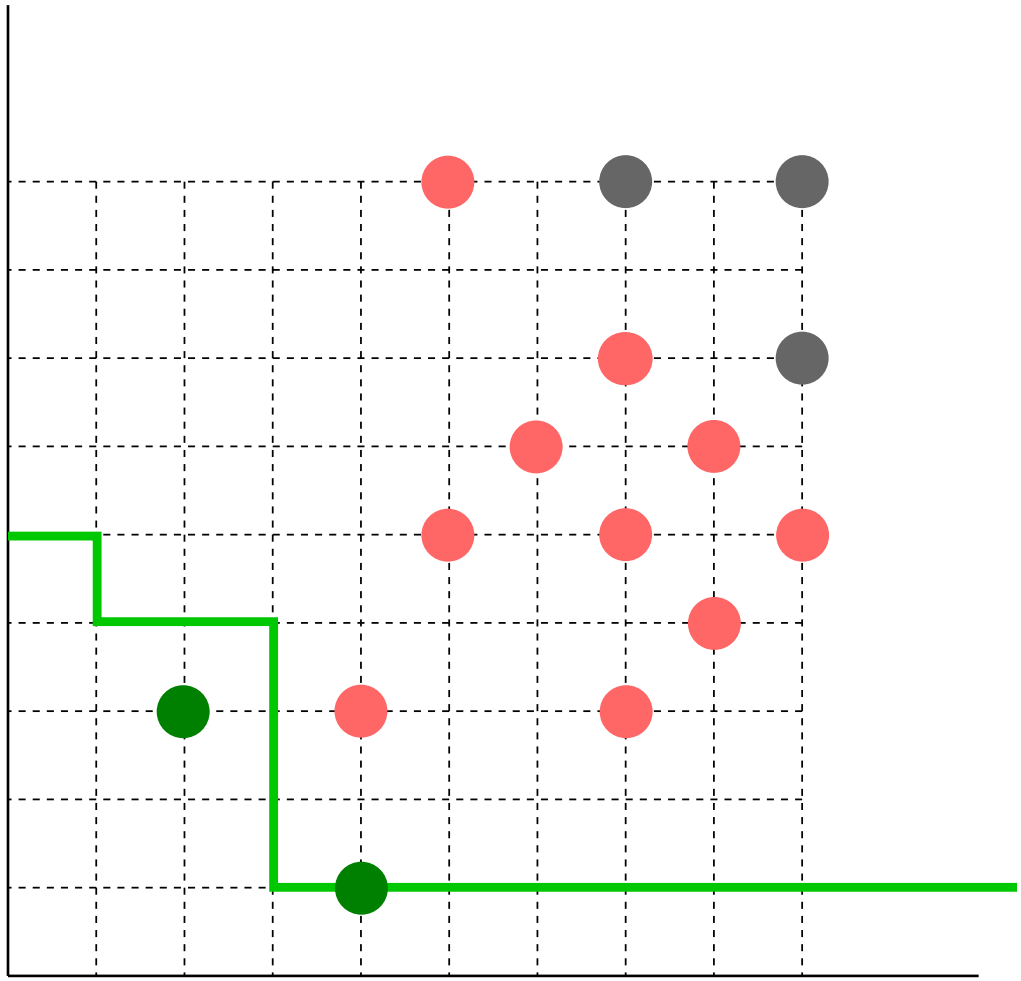
Обычный алгоритм редукции



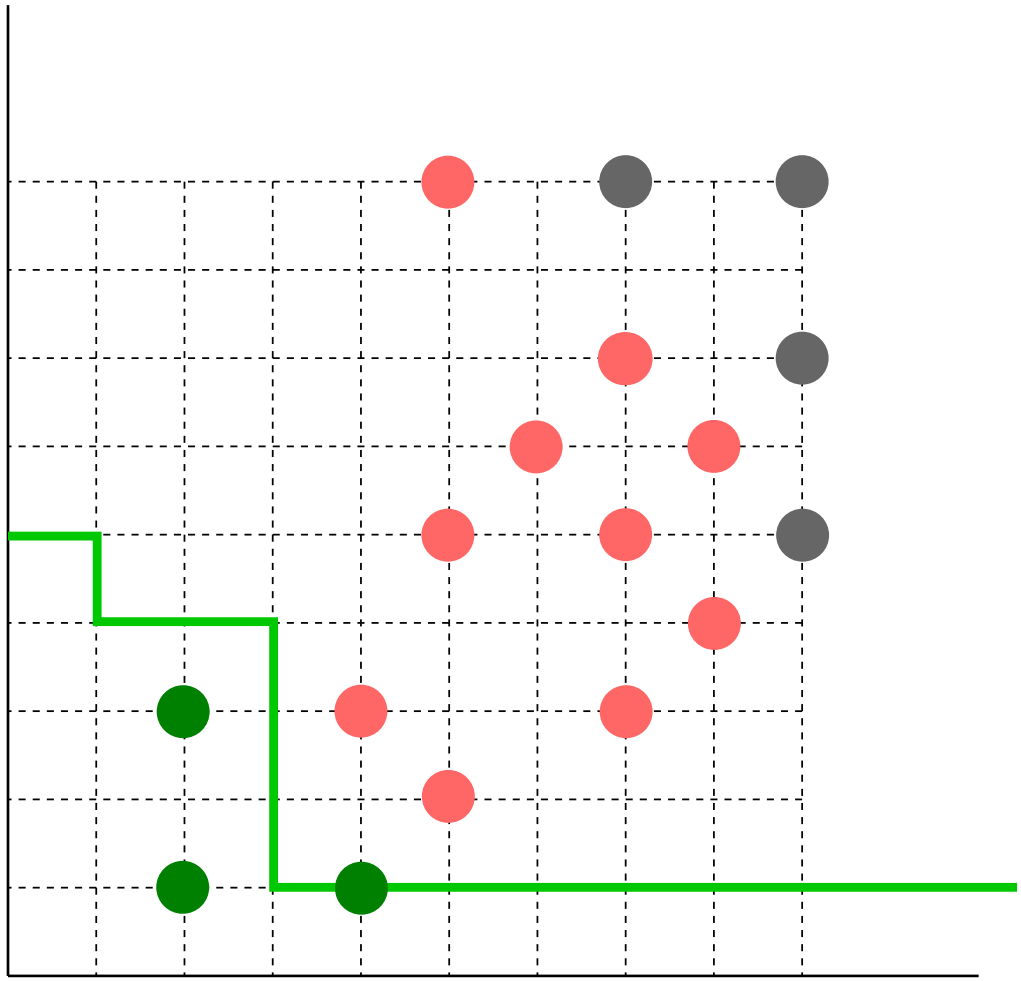
Обычный алгоритм редукции



Обычный алгоритм редукции



Обычный алгоритм редукции



Метод РСВП

$$N(\lambda p + \mu q) = \lambda N(p) + \mu N(q)$$
$$N(p \cdot q) = N(N(p) \cdot N(q))$$

- Вычисляет нормальную форму снизу вверх

Метод РСВП

$$N(\lambda p + \mu q) = \lambda N(p) + \mu N(q)$$

$$N(p \cdot q) = N(N(p) \cdot N(q))$$

- Вычисляет нормальную форму снизу вверх
- Сохраняет нормальные формы мономов

Метод РСВП

$$N(\lambda p + \mu q) = \lambda N(p) + \mu N(q)$$
$$N(p \cdot q) = N(N(p) \cdot N(q))$$

- Вычисляет нормальную форму снизу вверх
- Сохраняет нормальные формы мономов
- Нормальная форма каждого монома вычисляется лишь единожды

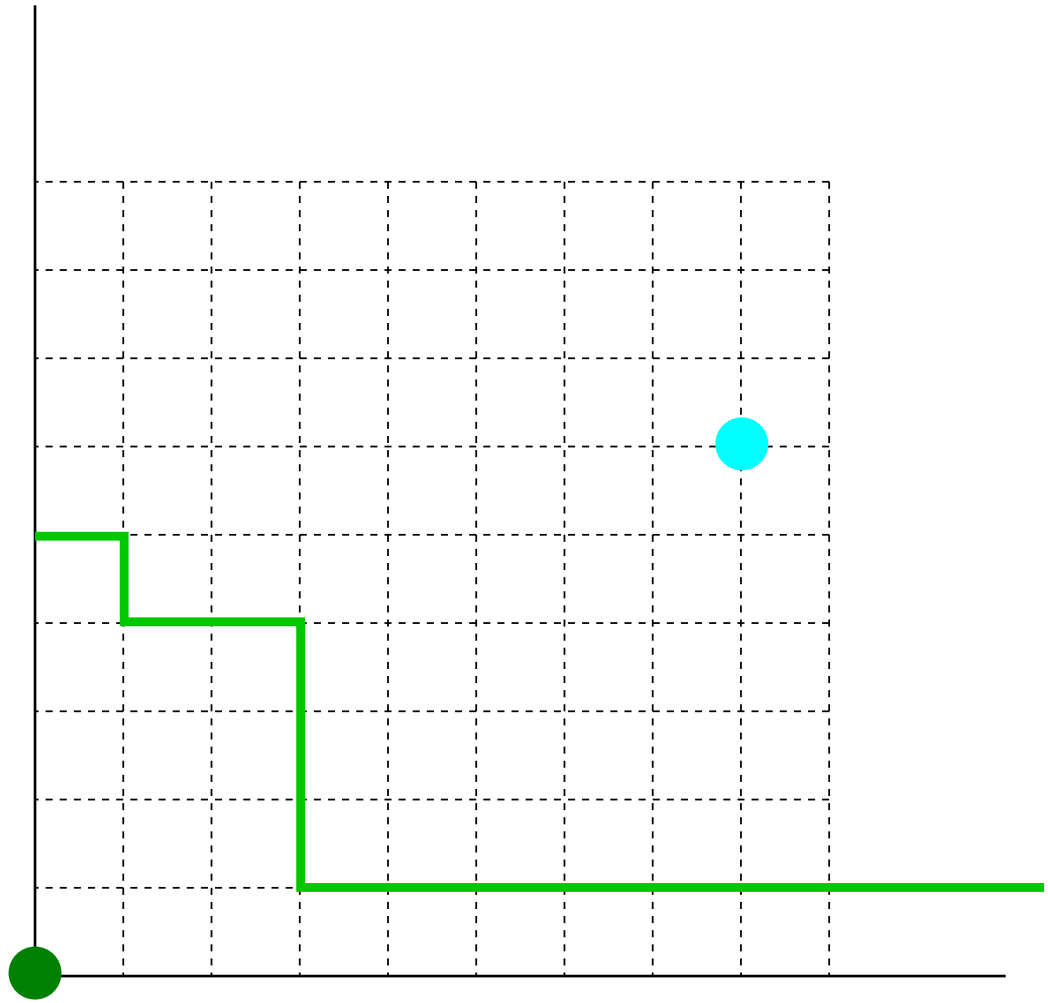
Метод РСВП

$$N(\lambda p + \mu q) = \lambda N(p) + \mu N(q)$$

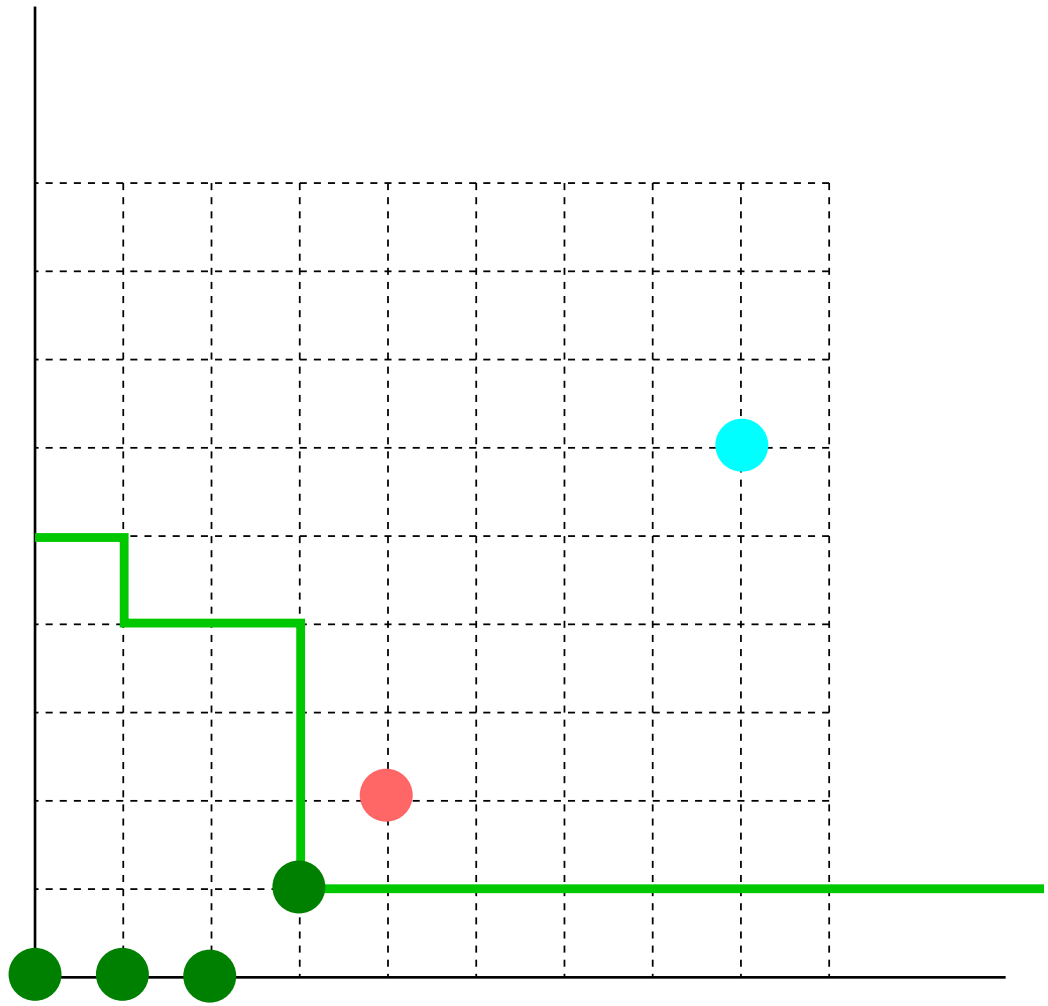
$$N(p \cdot q) = N(N(p) \cdot N(q))$$

- Вычисляет нормальную форму снизу вверх
- Сохраняет нормальные формы мономов
- Нормальная форма каждого монома вычисляется лишь единожды
- Сокращается число промежуточных членов

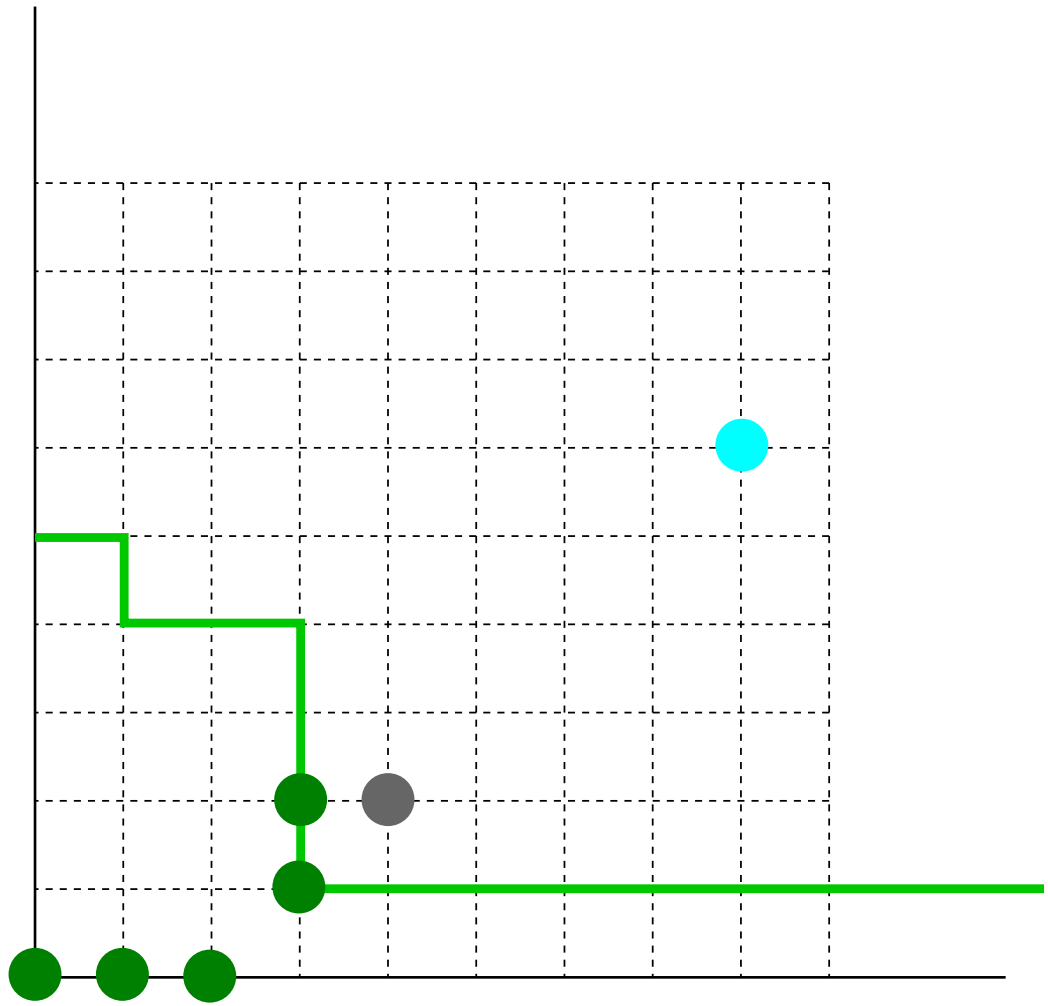
Динамика редукции по методу РСВП



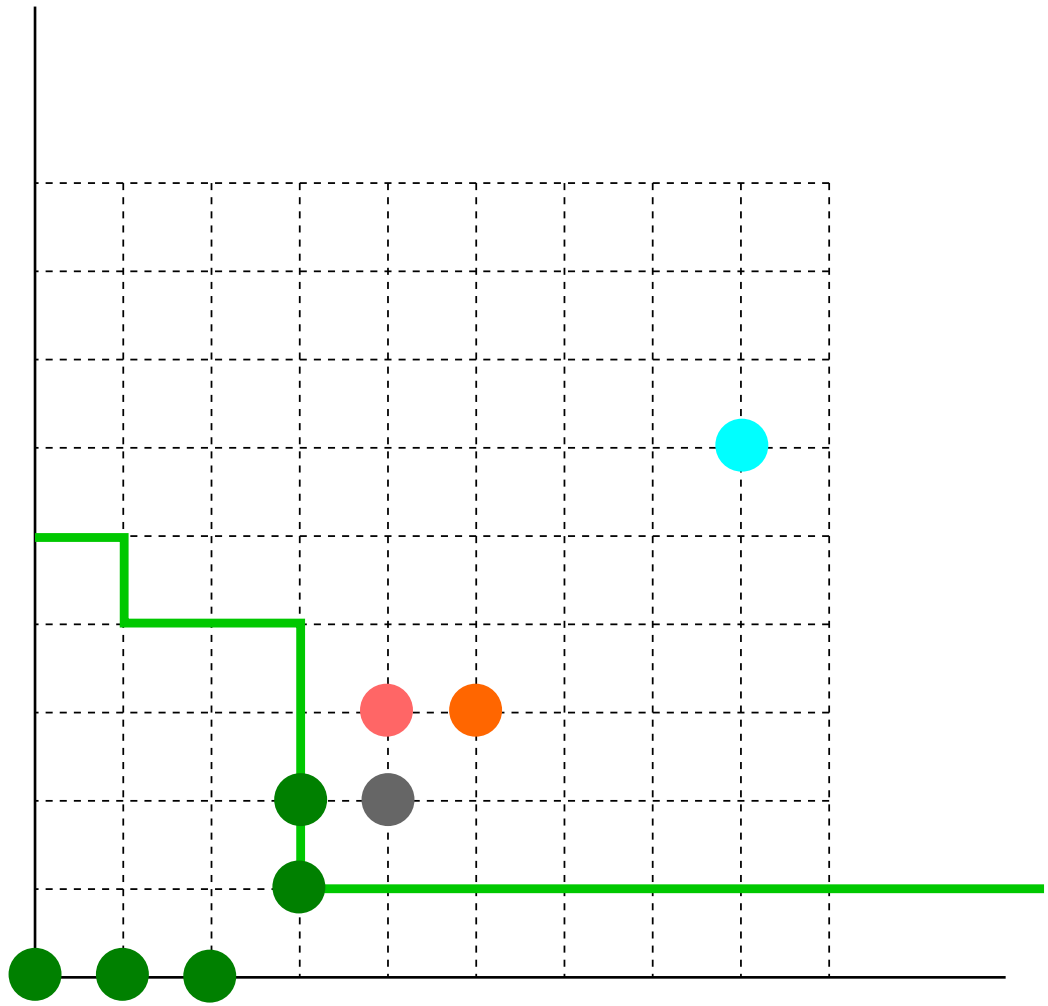
Динамика редукции по методу РСВП



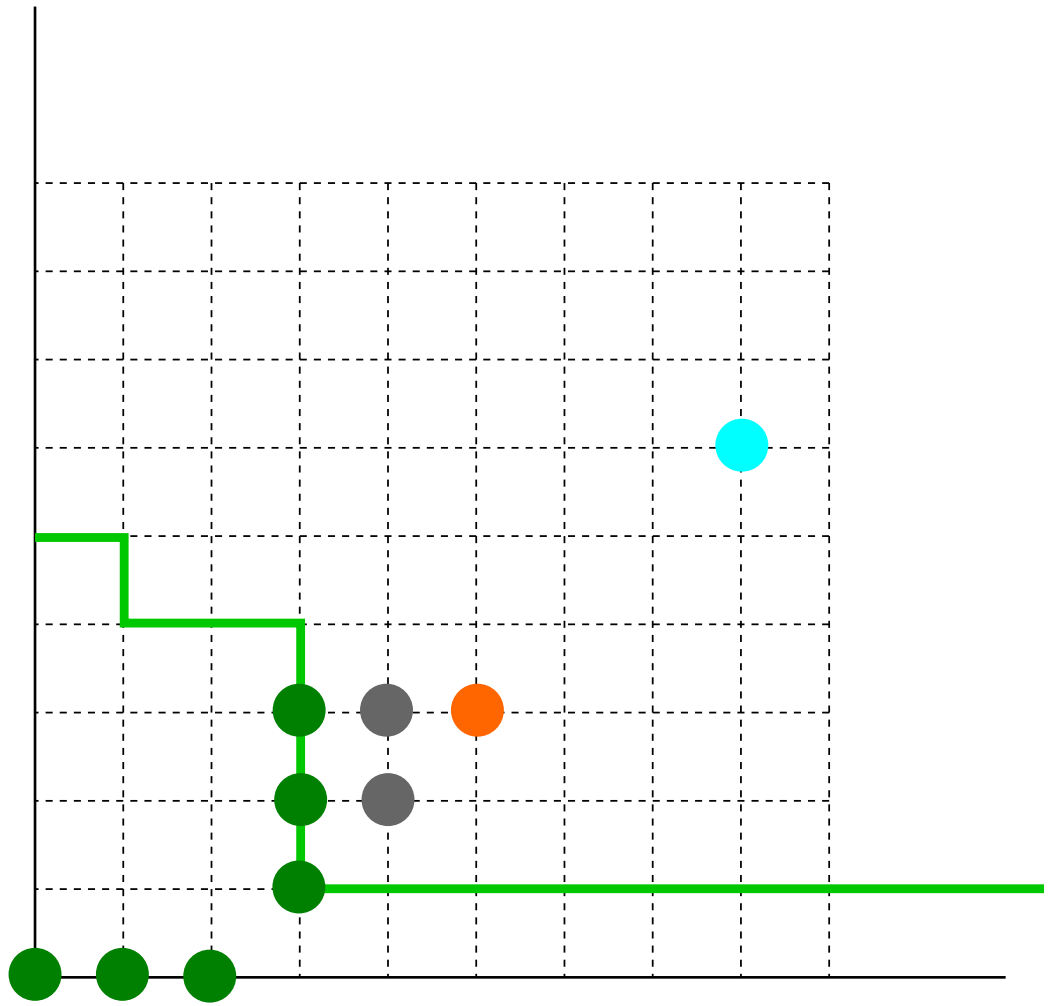
Динамика редукции по методу РСВП



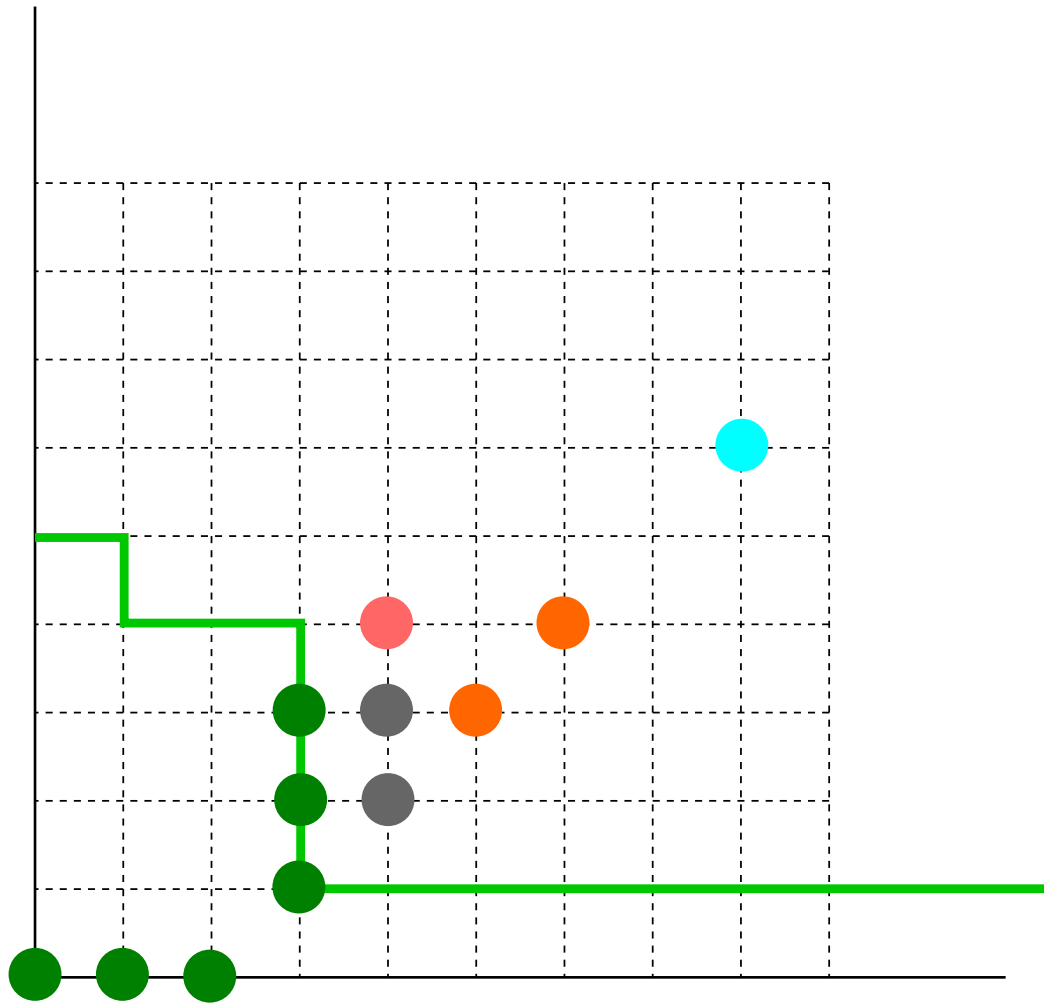
Динамика редукции по методу РСВП



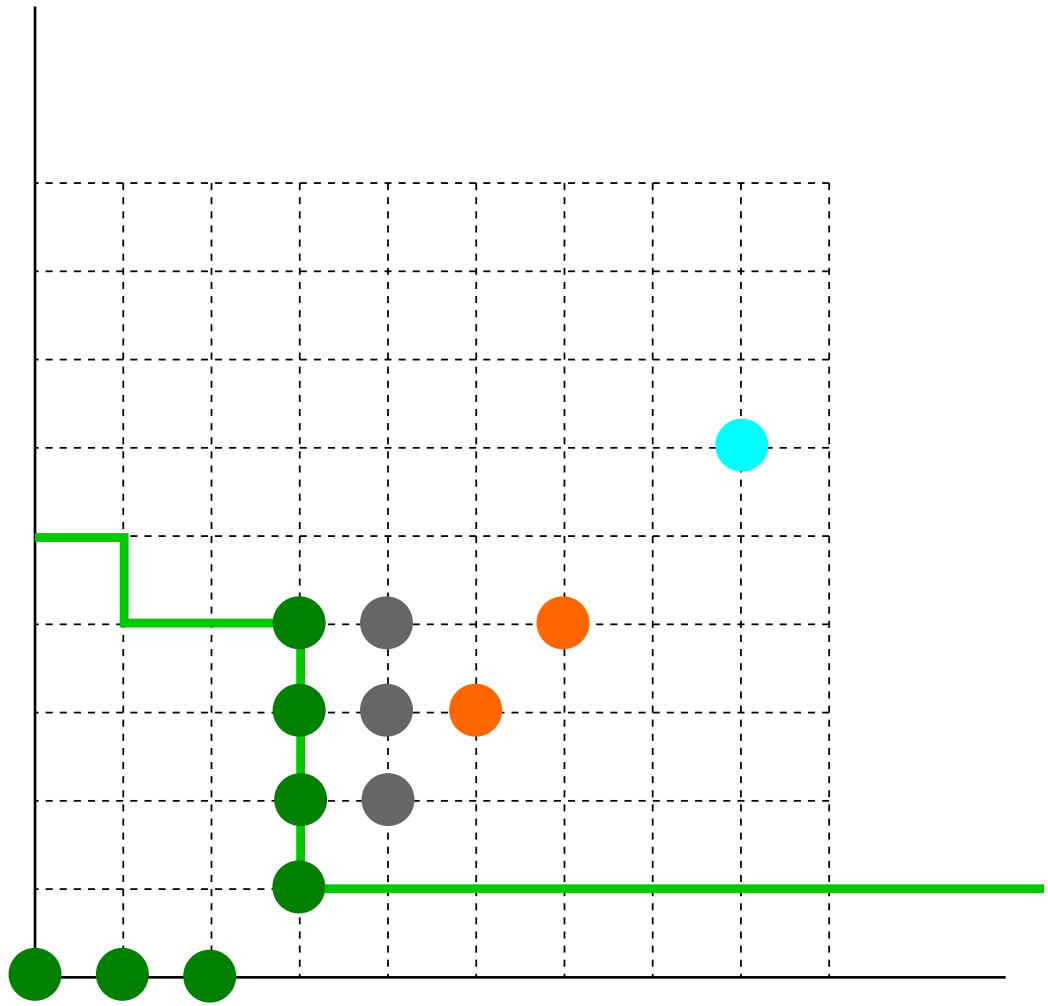
Динамика редукции по методу РСВП



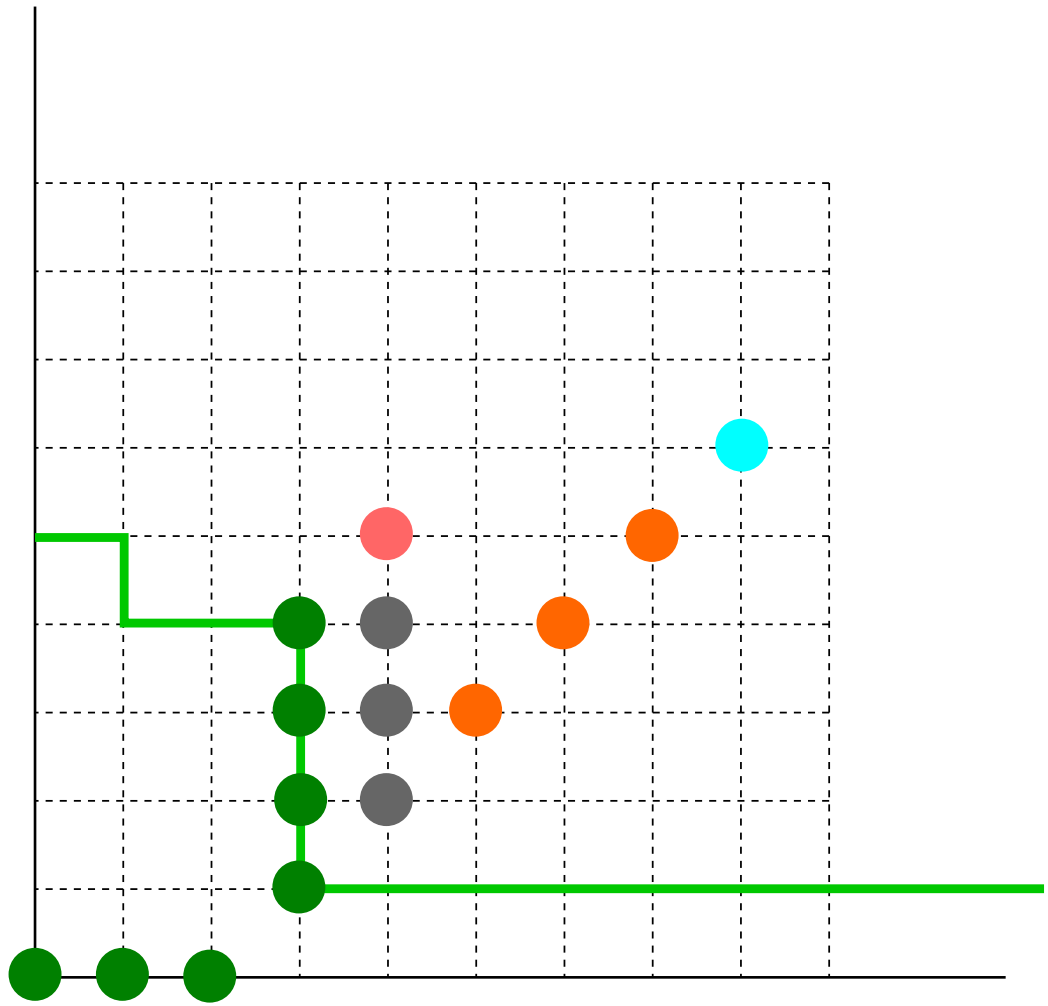
Динамика редукции по методу РСВП



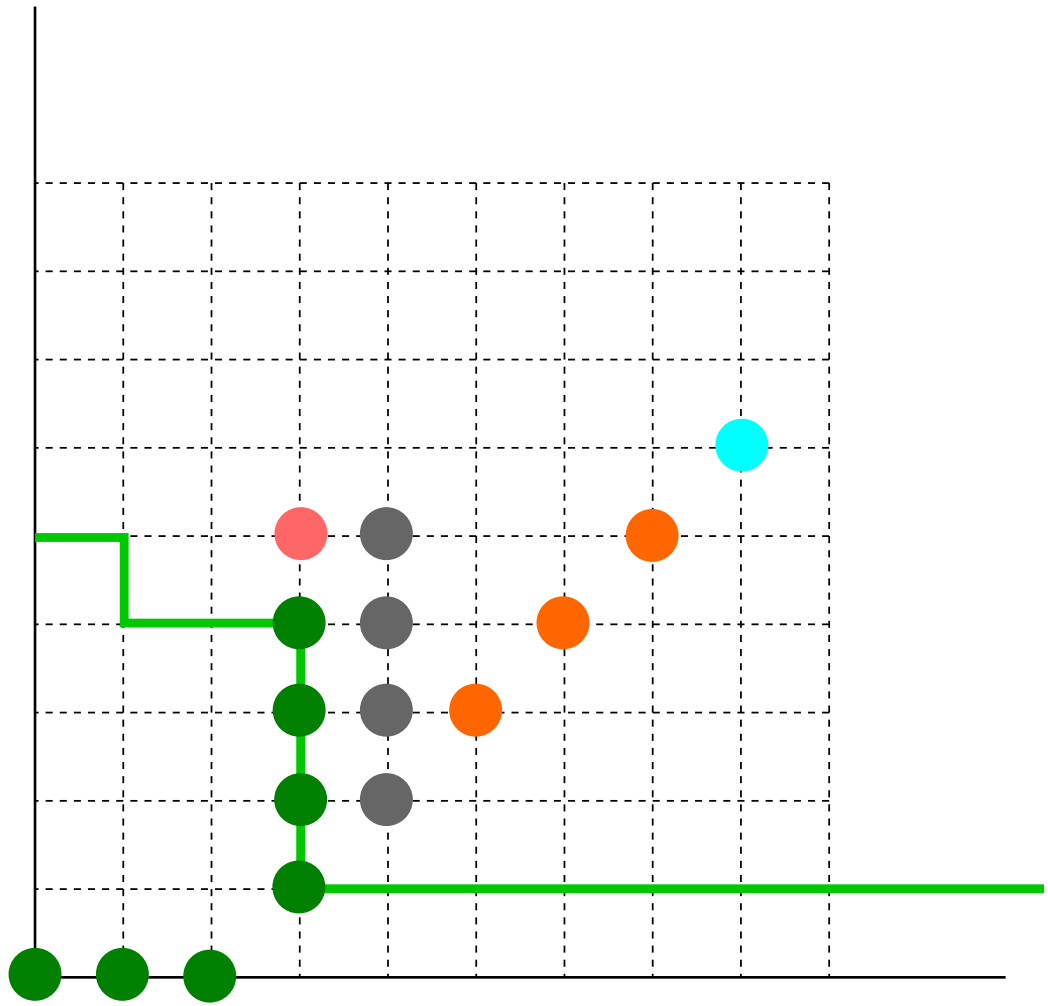
Динамика редукции по методу РСВП



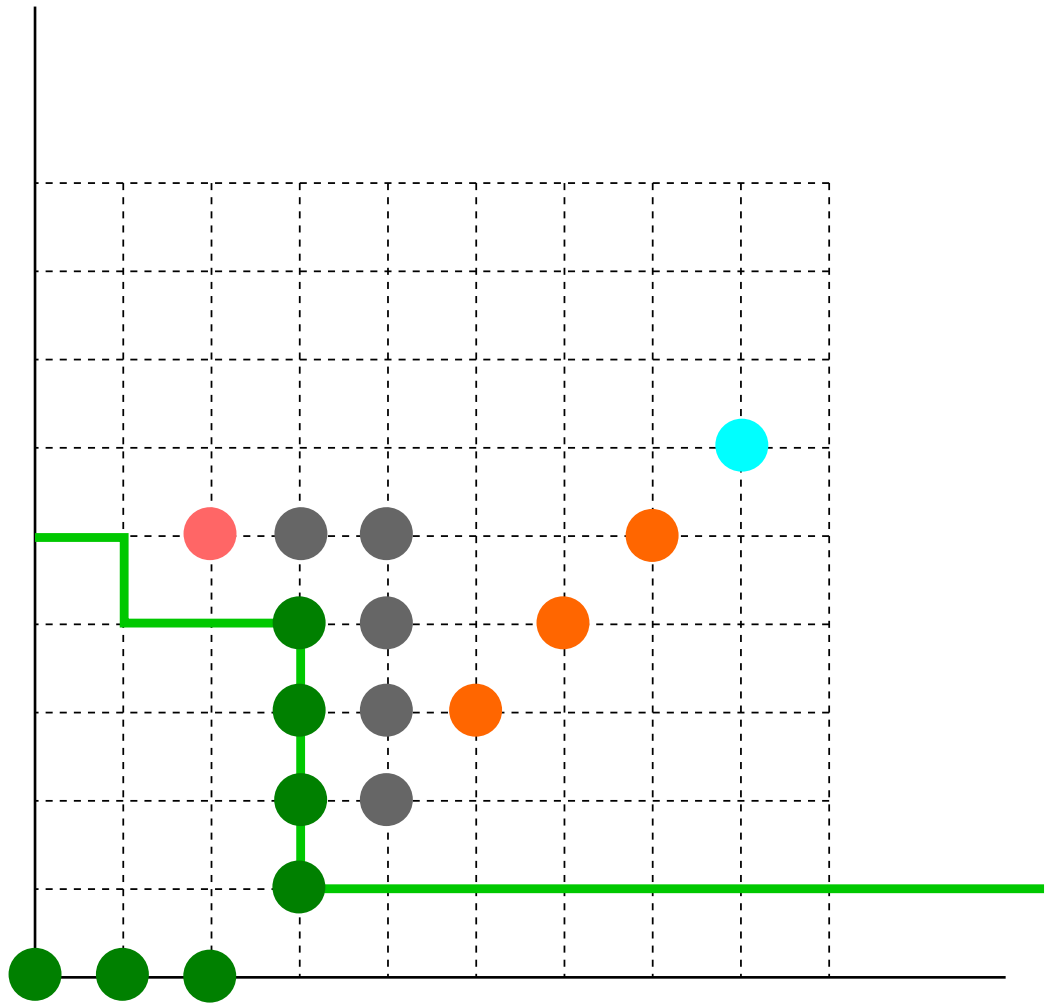
Динамика редукции по методу РСВП



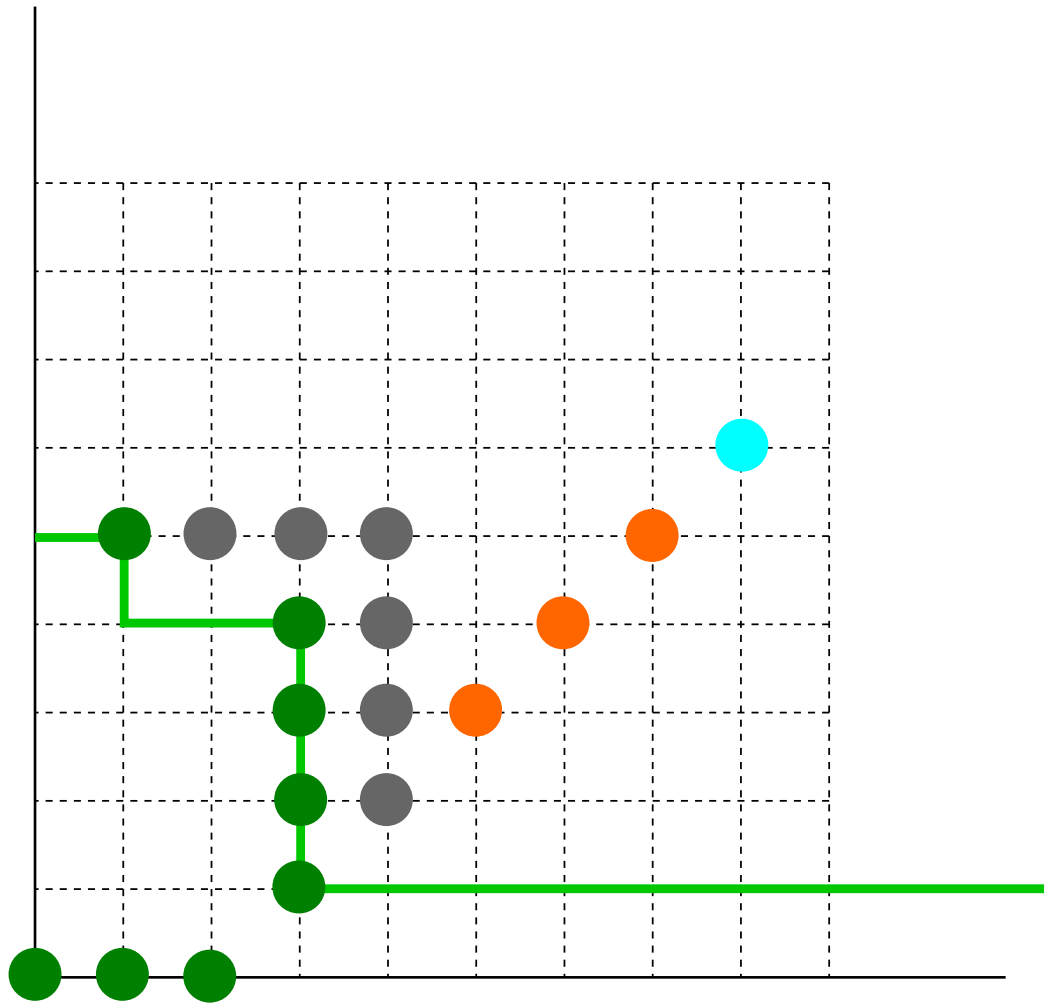
Динамика редукции по методу РСВП



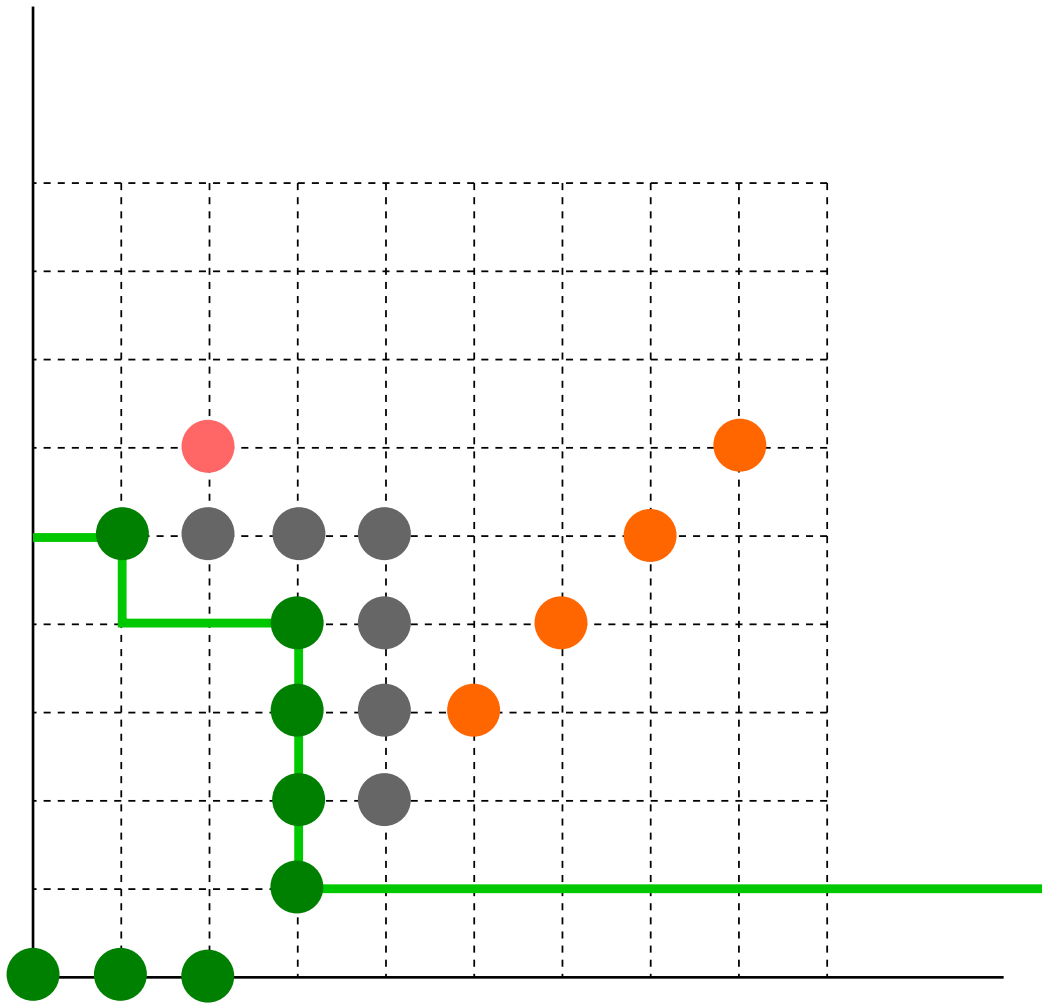
Динамика редукции по методу РСВП



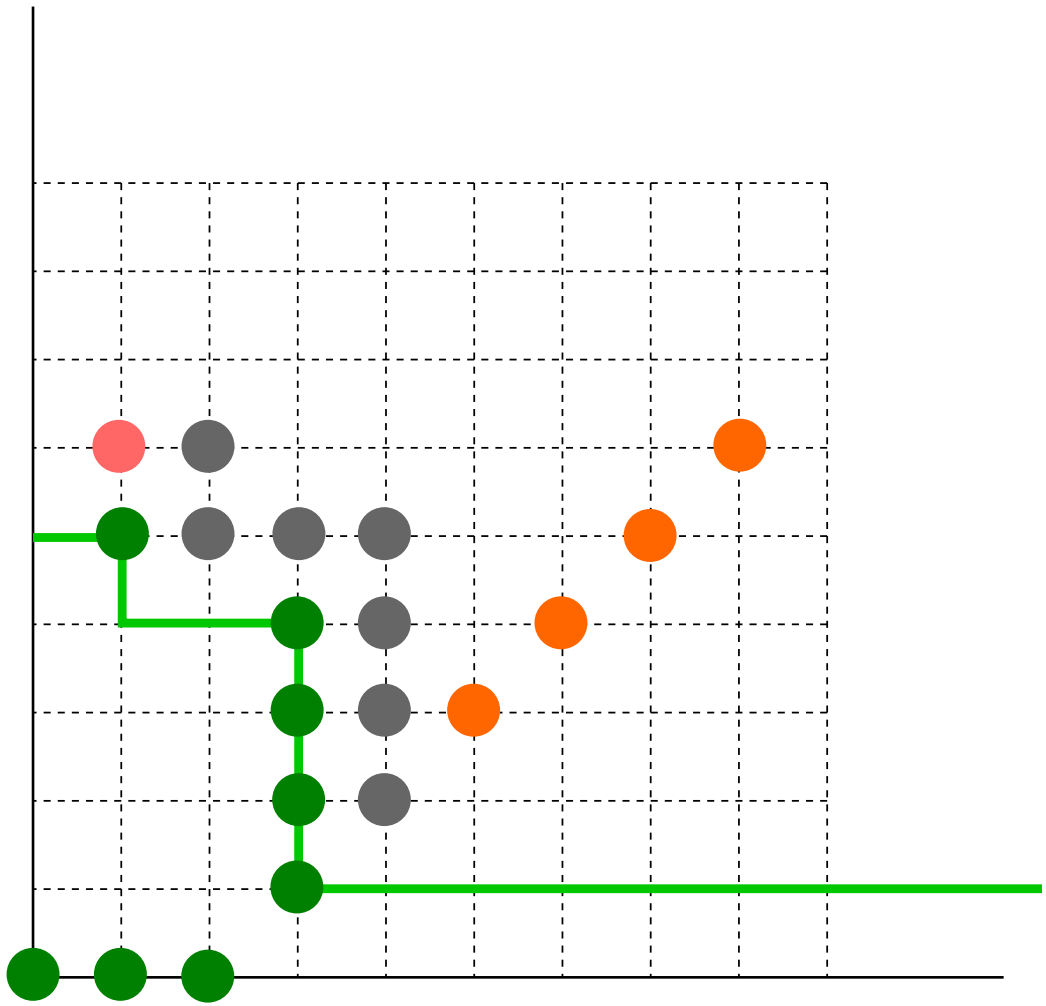
Динамика редукции по методу РСВП



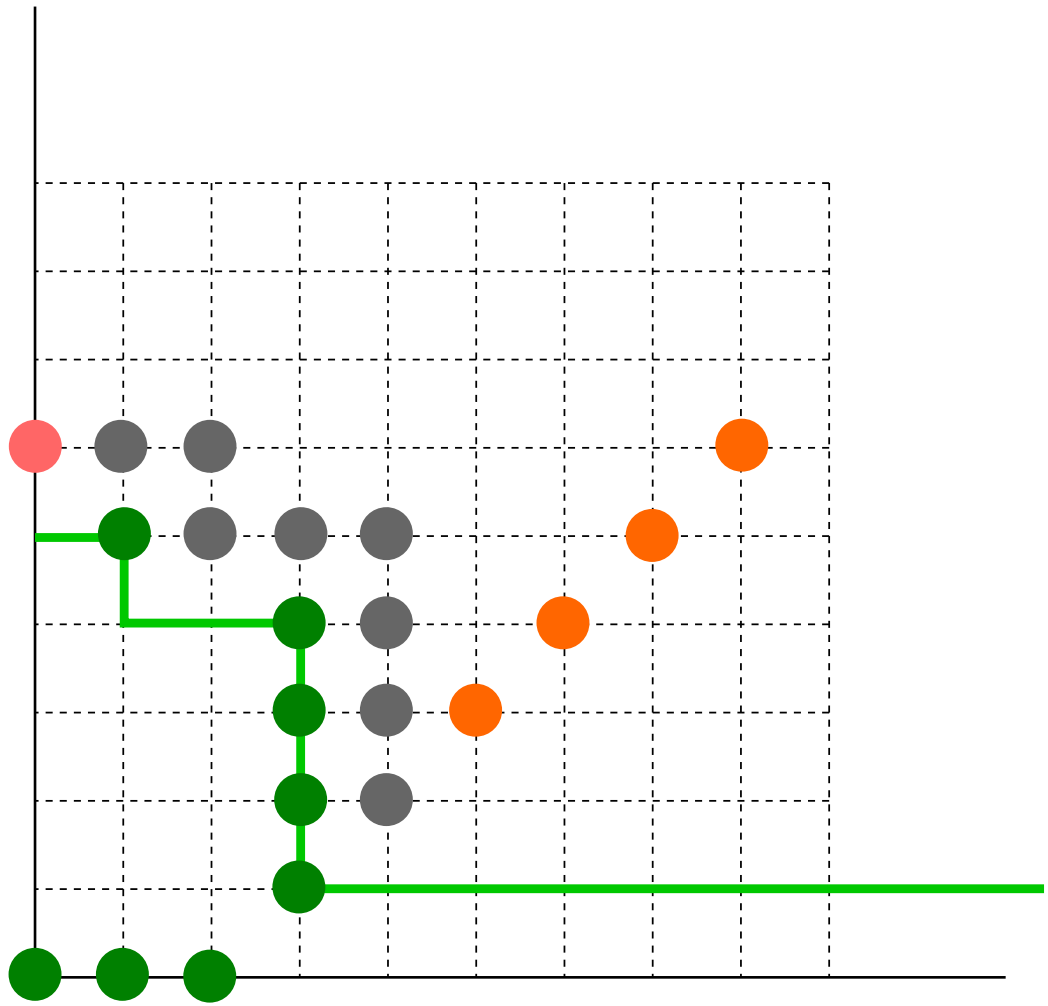
Динамика редукции по методу РСВП



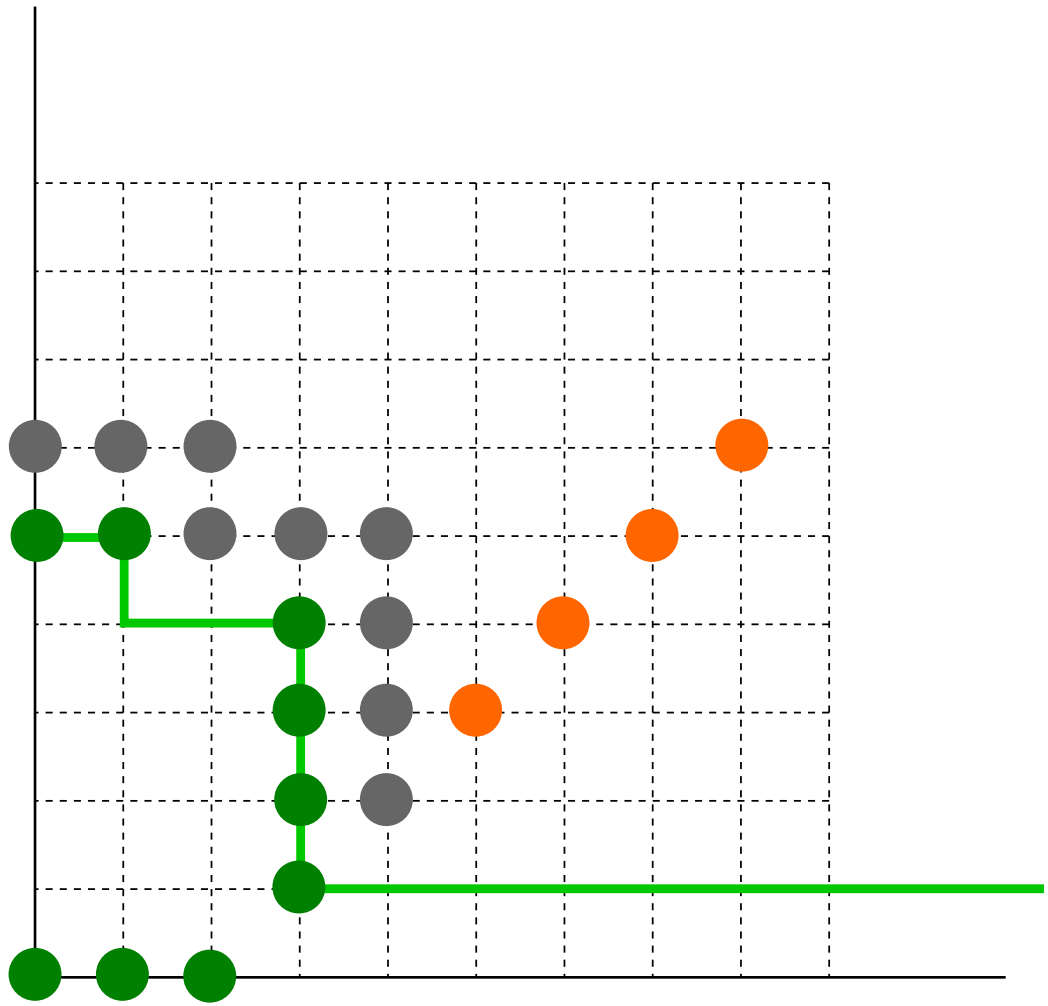
Динамика редукции по методу РСВП



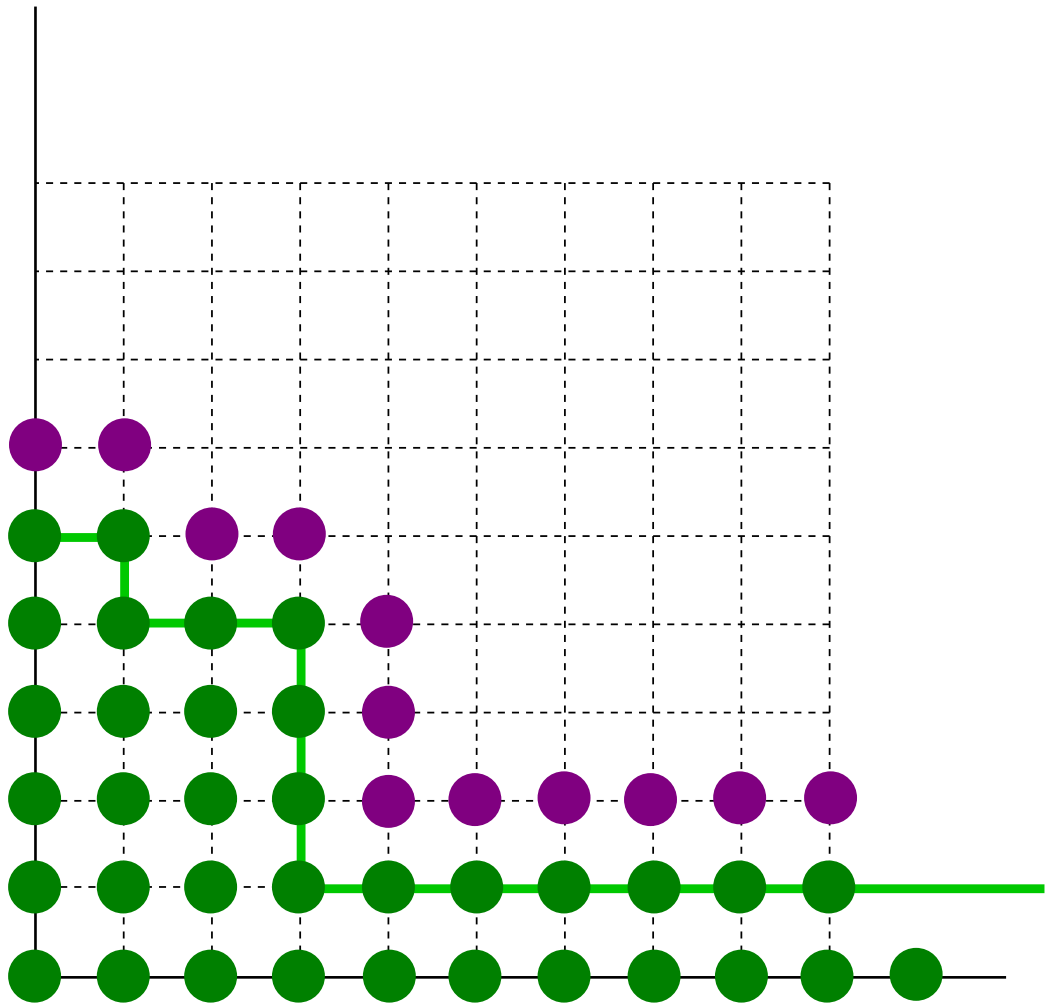
Динамика редукции по методу РСВП



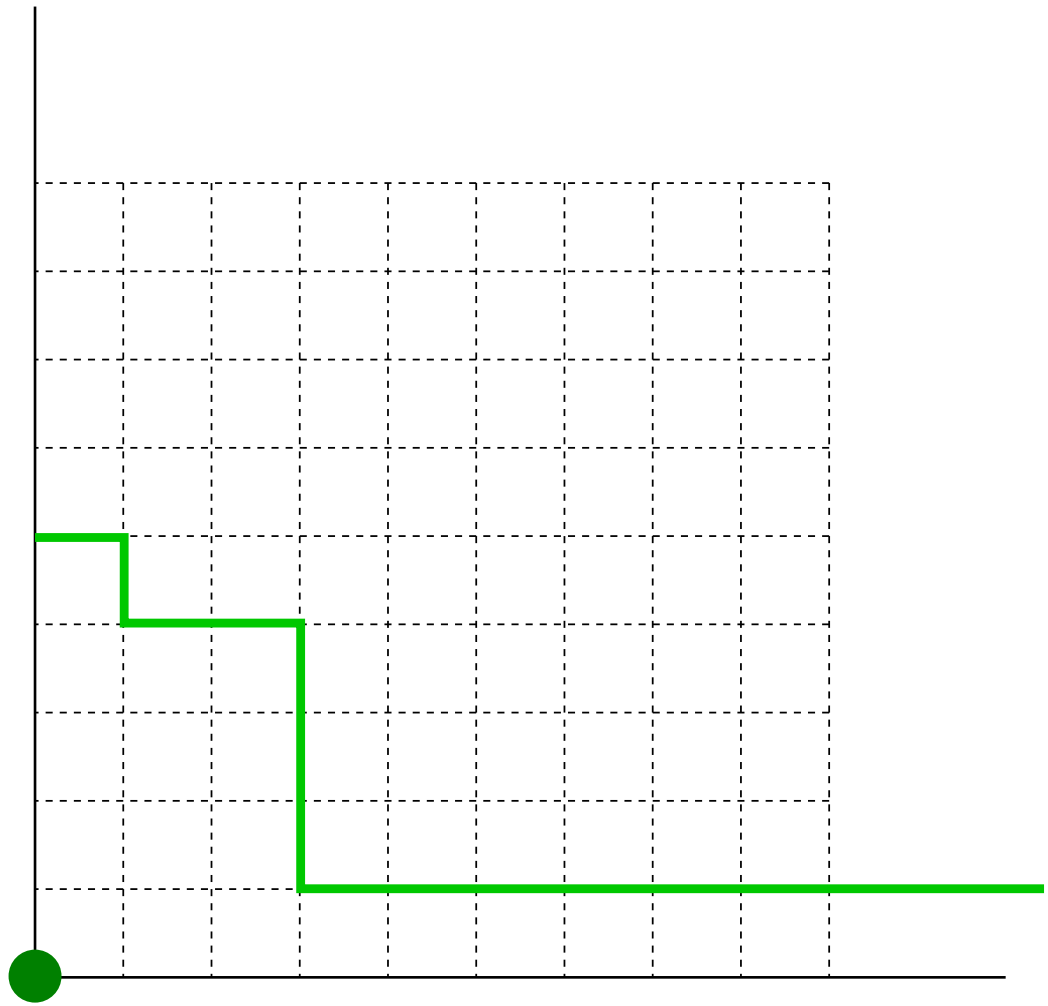
Динамика редукции по методу РСВП



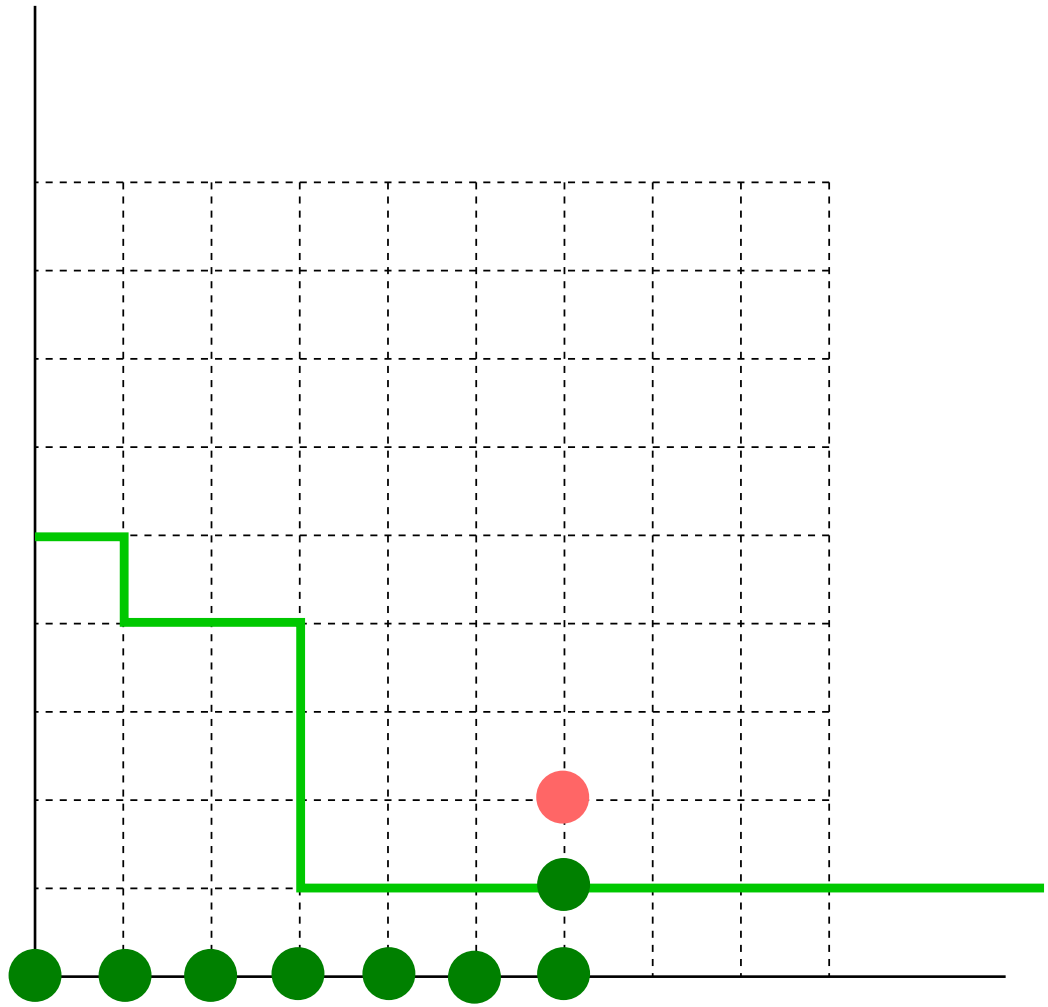
Достаточное множество мономов



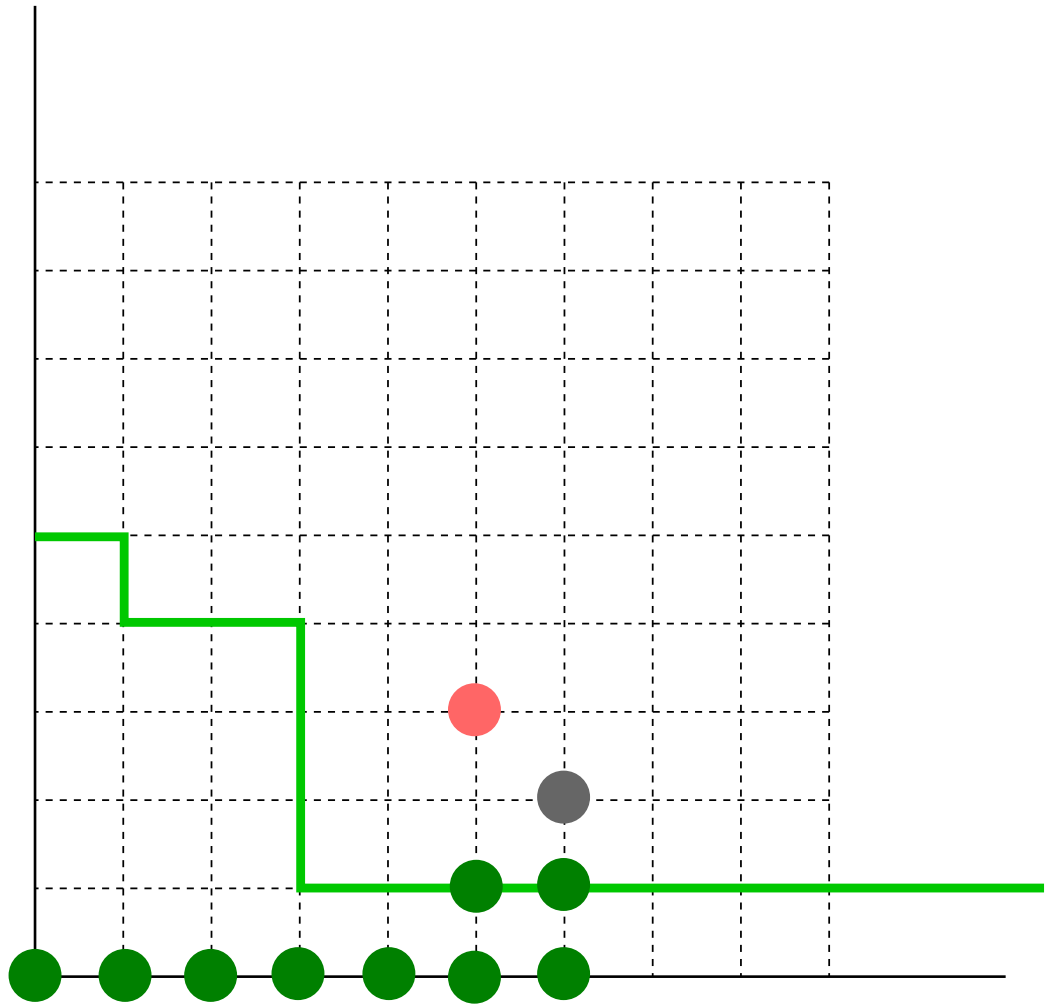
Динамика редукции по методу РСВП



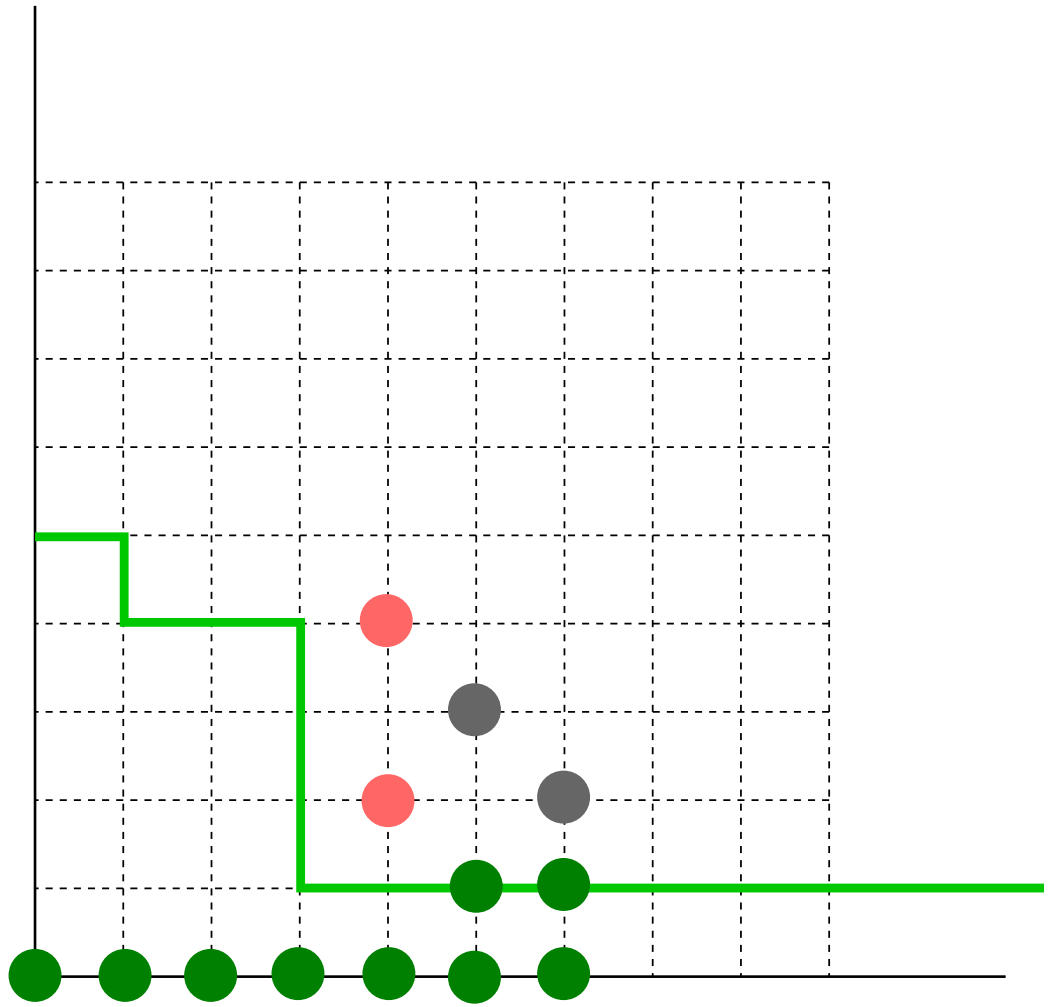
Динамика редукции по методу РСВП



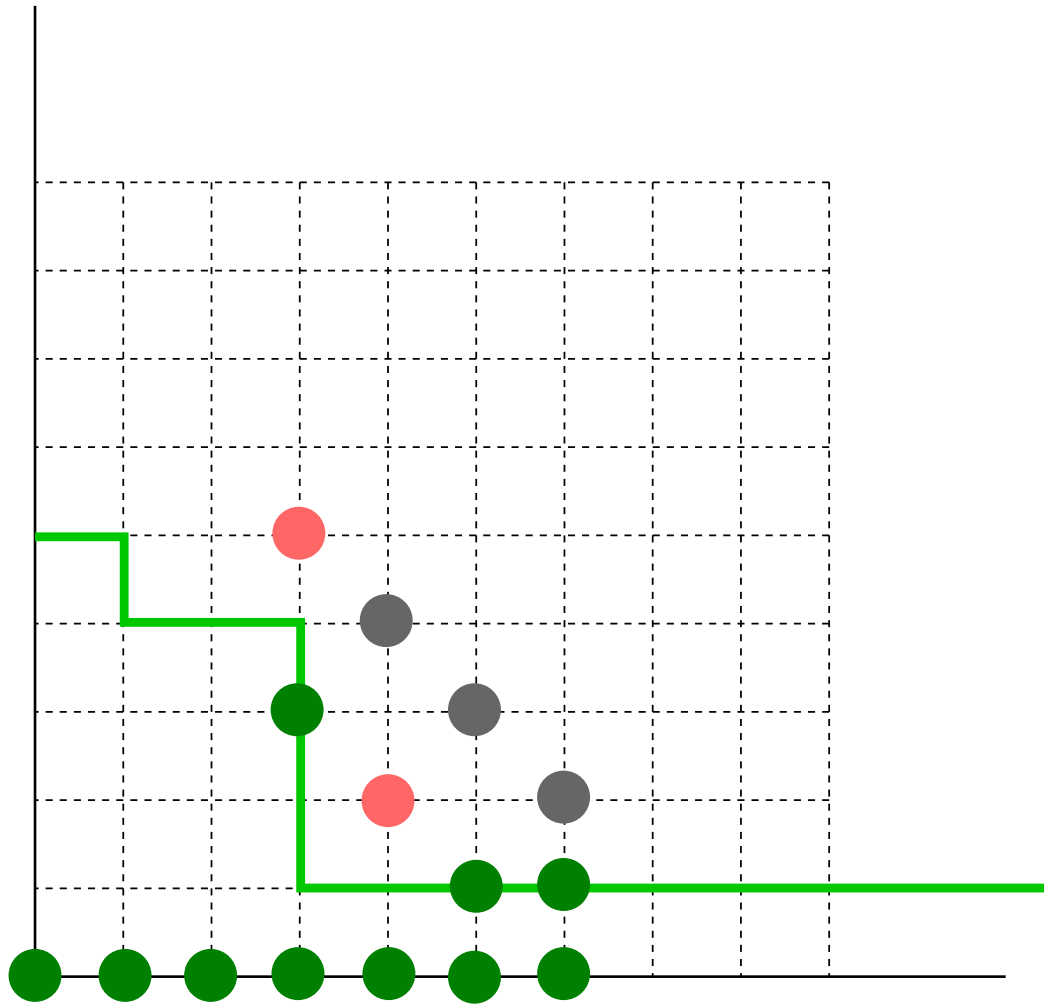
Динамика редукции по методу РСВП



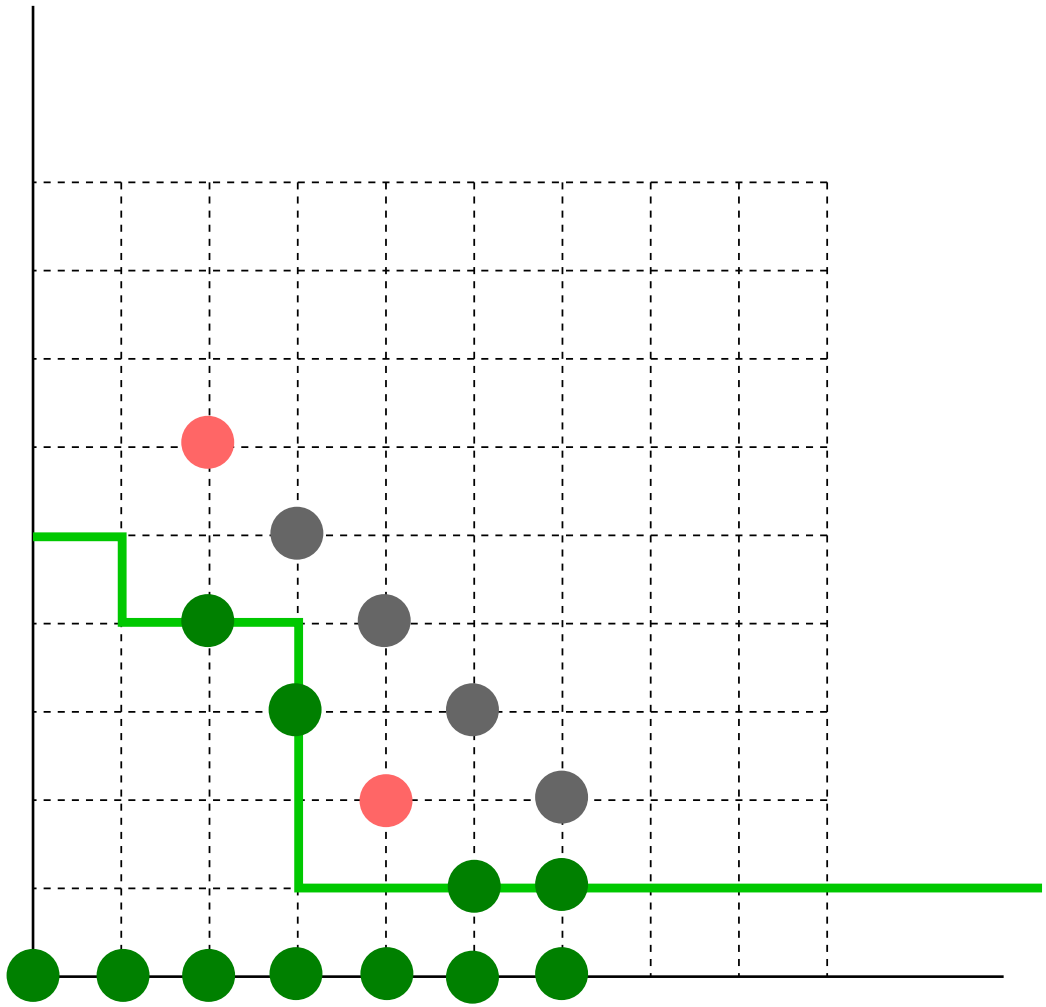
Динамика редукции по методу РСВП



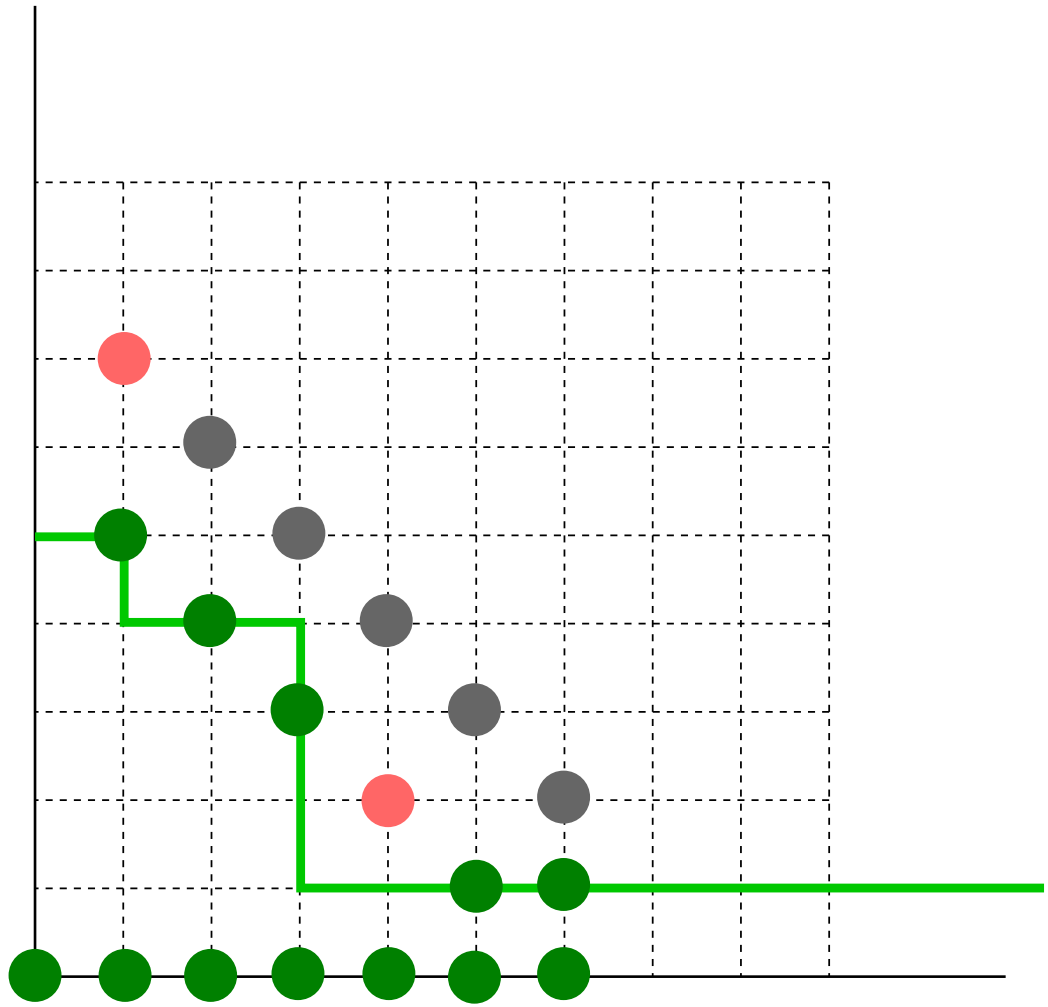
Динамика редукции по методу РСВП



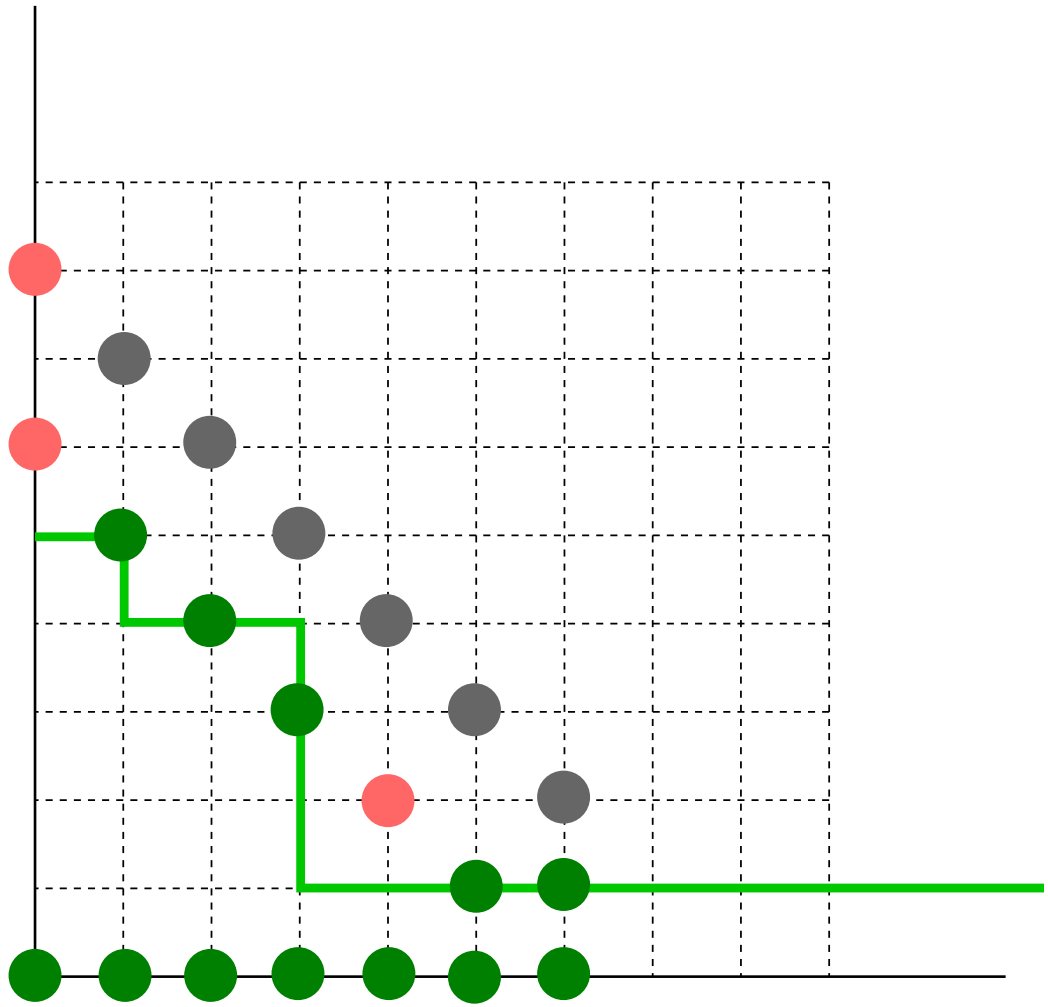
Динамика редукции по методу РСВП



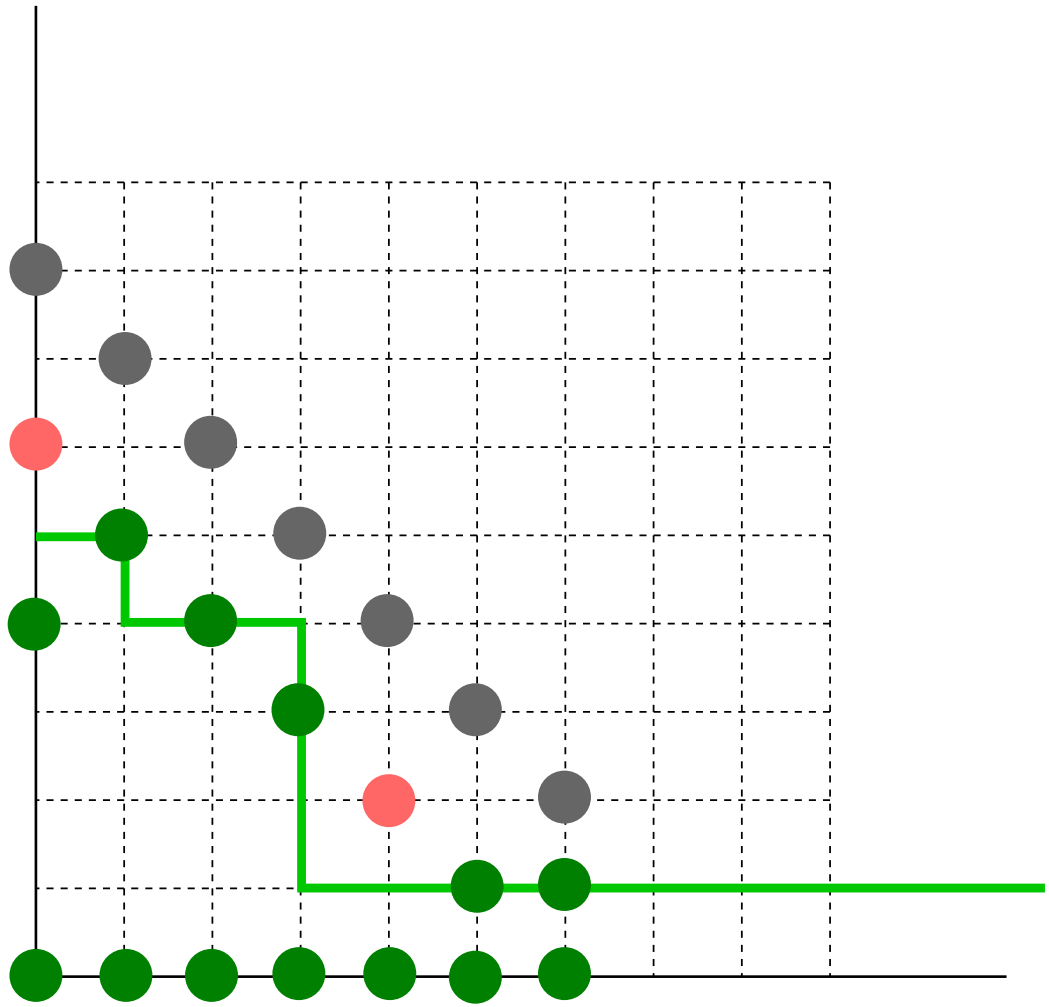
Динамика редукции по методу РСВП



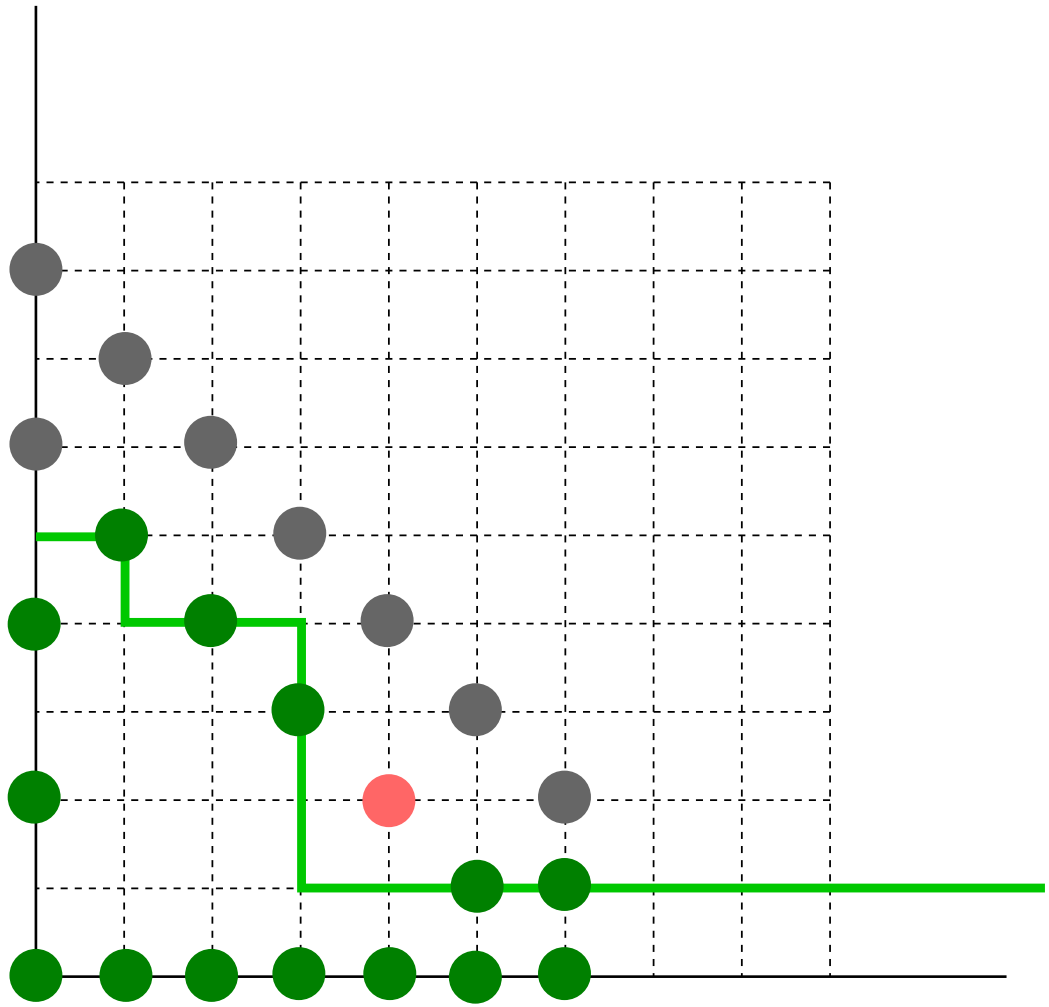
Динамика редукции по методу РСВП



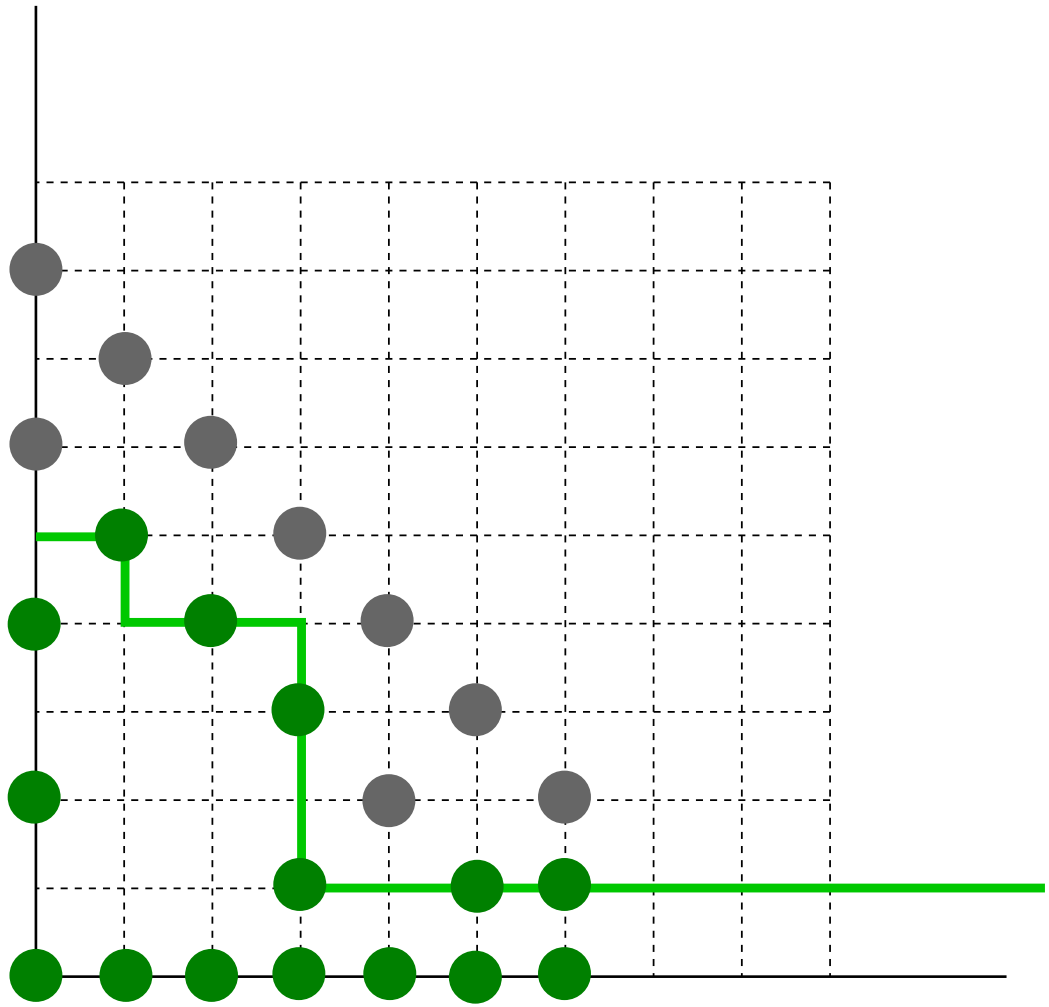
Динамика редукции по методу РСВП



Динамика редукции по методу РСВП



Динамика редукции по методу РСВП



Метод РСВП

Эффективность зависит от используемой схемы

Методы построения схем

- Тривиальная схема

Методы построения схем

- Тривиальная схема
- Обобщенный метод Горнера

Методы построения схем

- Тривиальная схема
- Обобщенный метод Горнера
- Метод «минимального покрывающего дерева» (ММПД)

Метод Горнера

$$p \to mq + r$$

Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$

Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$
- $x(x^3 + x^2y^2 + x + y^2) + y^2 + y^4 + y^5$

Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$
- $x(x^3 + x^2y^2 + x + y^2) + y^2 + y^4 + y^5$
- $x(x(x^2 + xy^2 + 1) + y^2) + y^2 + y^4 + y^5$

Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$
- $x(x^3 + x^2y^2 + x + y^2) + y^2 + y^4 + y^5$
- $x(x(x^2 + xy^2 + 1) + y^2) + y^2 + y^4 + y^5$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2 + y^4 + y^5$

Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$
- $x(x^3 + x^2y^2 + x + y^2) + y^2 + y^4 + y^5$
- $x(x(x^2 + xy^2 + 1) + y^2) + y^2 + y^4 + y^5$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2 + y^4 + y^5$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2(1 + y^2 + y^3)$

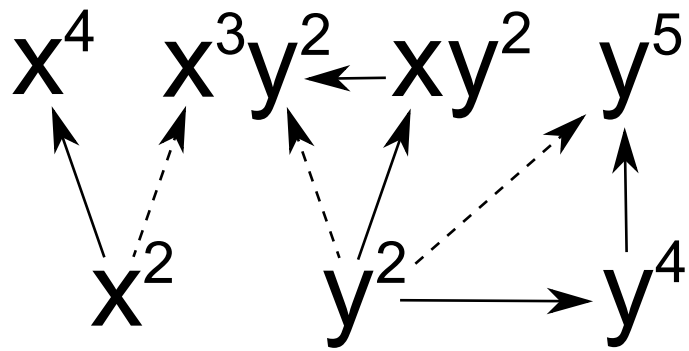
Метод Горнера

$$p \to mq + r$$

- $x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$
- $x(x^3 + x^2y^2 + x + y^2) + y^2 + y^4 + y^5$
- $x(x(x^2 + xy^2 + 1) + y^2) + y^2 + y^4 + y^5$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2 + y^4 + y^5$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2(1 + y^2 + y^3)$
- $x(x(x(1 + y^2) + 1) + y^2) + y^2(1 + y^2(1 + y))$

Метод «минимального покрывающего дерева»

$$x^4 + x^3y^2 + x^2 + xy^2 + y^2 + y^4 + y^5$$



- Минимальный остовный граф с заданными свойствами

Критерии качества схем

- Стоимость операций умножения существенно варьируется

Критерии качества схем

- Стоимость операций умножения существенно варьируется
- Ее нельзя с достаточной точностью предсказать заранее

Критерии качества схем

- Стоимость операций умножения существенно варьируется
- Ее нельзя с достаточной точностью предсказать заранее
- Сложность редукции не связана с ее результатом

Критерии качества схем

- Стоимость операций умножения существенно варьируется
- Ее нельзя с достаточной точностью предсказать заранее
- Сложность редукции не связана с ее результатом
- Равномерный критерий качества не отвечает нашим требованиям

Критерии качества схем

- Стоимость операций умножения существенно варьируется
- Ее нельзя с достаточной точностью предсказать заранее
- Сложность редукции не связана с ее результатом
- Равномерный критерий качества не отвечает нашим требованиям
- Поиск оптимальной схемы не нужен

Детали реализации

- Прототип на `Python`

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP
- Юнит-тесты

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP
- Юнит-тесты

Особенности:

- Каждому моному присваивается уникальный идентификатор

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP
- Юнит-тесты

Особенности:

- Каждому моному присваивается уникальный идентификатор
- Полиномы – списки с общим пулом элементов

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP
- Юнит-тесты

Особенности:

- Каждому моному присваивается уникальный идентификатор
- Полиномы – списки с общим пулом элементов
- Коэффициенты из поля рациональных чисел или конечного поля

Детали реализации

- Прототип на `Python`
- Реализация на кроссплатформенном C++ с использованием GMP
- Юнит-тесты

Особенности:

- Каждому моному присваивается уникальный идентификатор
- Полиномы – списки с общим пулом элементов
- Коэффициенты из поля рациональных чисел или конечного поля
- Исключается повторное вычисление нормальной формы мономов

Методология тестирования

- Тестирование на отдельных примерах

Методология тестирования

- Тестирование на отдельных примерах
- Сравнение с Maple 13

Методология тестирования

- Тестирование на отдельных примерах
- Сравнение с Maple 13
- Особенности редукции над $\mathbb{Q}$

Схемы с точки зрения равномерного критерия

Количество операций умножения:

	ТС	МГ	ММПД
p_1	8684	**1221**	2995
p_2	39246	**6865**	10345
p_3	121796	**34361**	41772

Метод Горнера показывает наилучшие результаты благодаря возможности добавления узлов

Редукция полиномов над $\mathbb{Q}$

Время редукции, мс:

	ТС	МГ	ММПД	Maple
p_1	827	**187**	684	3270
p_2	1863	**320**	520	15868
p_3	210557	**75846**	127671	391264

Редукция полиномов над $GF(31)$

Время редукции, мс:

	ТС	МГ	ММПД	Maple
q_1	**34**	62	150	3716
q_2	2908	5552	**2366**	1674390
q_3	**25183**	65732	39224	–

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,
- допускает частично параллельную реализацию,

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,
- допускает частично параллельную реализацию,
- позволяет редуцировать несколько полиномов совместно.

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,
- допускает частично параллельную реализацию,
- позволяет редуцировать несколько полиномов совместно.

Однако,

- равномерный критерий сложности не отвечает фактической сложности,

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,
- допускает частично параллельную реализацию,
- позволяет редуцировать несколько полиномов совместно.

Однако,

- равномерный критерий сложности не отвечает фактической сложности,
- схема, построенная заранее, может быть сколь угодно далека от оптимальной,

Выводы

Метод РСВП

- обладает высокой гибкостью и эффективностью,
- допускает частично параллельную реализацию,
- позволяет редуцировать несколько полиномов совместно.

Однако,

- равномерный критерий сложности не отвечает фактической сложности,
- схема, построенная заранее, может быть сколь угодно далека от оптимальной,
- направление подъема существенно влияет на эффективность алгоритма.

Дальше

Для повышения эффективности данного подхода необходимо

- строить схему в процессе редукции,

Дальше

Для повышения эффективности данного подхода необходимо

- строить схему в процессе редукции,
- тщательно выбирать направление подъема,

Дальше

Для повышения эффективности данного подхода необходимо

- строить схему в процессе редукции,
- тщательно выбирать направление подъема,
- добавлять промежуточные мономы лишь если они мало отклоняются от заданного направления.

Дальше

Для повышения эффективности данного подхода необходимо

- строить схему в процессе редукции,
- тщательно выбирать направление подъема,
- добавлять промежуточные мономы лишь если они мало отклоняются от заданного направления.

Также необходимо исследовать эффективность данного алгоритма в при работе с булевыми полиномами и другими полиномами высокой размерности.

Заключение

- Выполнена эффективная реализация РСВП

Заключение

- Выполнена эффективная реализация РСВП
- Рассмотрены различные методы создания СВП и их эффективность в контексте РСВП

Заключение

- Выполнена эффективная реализация РСВП
- Рассмотрены различные методы создания СВП и их эффективность в контексте РСВП
- Выполнено сравнение с современной системой компьютерной алгебры

Заключение

- Выполнена эффективная реализация РСВП
- Рассмотрены различные методы создания СВП и их эффективность в контексте РСВП
- Выполнено сравнение с современной системой компьютерной алгебры
- Предложена модификация рассматриваемого подхода

Спасибо за внимание!

Полиномы

Полиномы над полем рациональных чисел:

	# пер.	Степень	# мономов	Размерность б.	Степень б.
p_1	2	374	45	4	11
p_2	2	1444	54	12	20
p_3	3	821	267	17	19

Полиномы над конечным полем $GF(31)$:

	# пер.	Степень	# мономов	Размерность б.	Степень б.
q_1	3	53	36	30	20
q_2	3	289	72	30	20
q_3	3	126	132	14	30