

УДК 512.74, 519.61, 519.683

О СУПЕРВЫЧИСЛЕНИЯХ, СВЯЗАННЫХ С ПОДХОДОМ ПЛАТОНОВА К ПРОБЛЕМЕ КРУЧЕНИЯ В ЯКОБИАНАХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ

(Работа выполнена при поддержке РФФИ, гранты №№12-01-0190, 13-01-12402)

М.М. Петрунин, научный сотрудник

(НИИСИ РАН, Нахимовский просп., 36, корп. 1, г. Москва, 117218, Россия, petrunin@niisi.ras.ru)

Аннотация. В настоящей статье описываются вычислительные аспекты нового подхода к нахождению фундаментальных единиц в гиперэллиптических полях, развитого в последние пять лет В.П. Платоновым (частично совместно с В.В. Беньяш-Кривецом). Естественная связь проблемы вычисления фундаментальных единиц с проблемой кручения в якобиевых многообразиях гиперэллиптических кривых над полем рациональных чисел позволила применить вычислительные методы и алгоритмы нахождения фундаментальных единиц в контексте проблемы кручения в якобианах. В данной статье рассматривается подход к организации супервычислений, связанных с указанным методом В.П. Платонова. Особый интерес представляет программная реализация алгоритмов, разработанная и оптимизированная для исполнения в гетерогенных вычислительных системах. Названные компьютерные вычисления позволили впервые после двенадцатилетнего перерыва найти точки кручения новых порядков.

Ключевые слова: фундаментальные единицы, гиперэллиптические поля, локально-глобальный принцип, якобиевы многообразия, гиперэллиптические кривые, проблема кручения в якобианах, быстрые алгоритмы, непрерывные дроби, компьютерная реализация, графические ускорители, OpenCL, оптимизация.

Терминология и изложение базисных результатов в данной работе соответствуют [1]. Пусть $f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ – свободный от квадратов многочлен. Через J_f обозначим якобиан (якобиево многообразие) гиперэллиптической кривой рода 2, определяемой уравнением $y^2 = f(x)$, а через $J_f(\mathbb{Q})$ – множество его точек, определенных над \mathbb{Q} . Уже более 30 лет остается открытой проблема существования такой константы C , что для любого f и любой точки конечного порядка $a \in J_f(\mathbb{Q})$ порядок точки a не превосходит C .

За это время не были найдены существенные идеи для решения данной проблемы, поэтому усилия исследователей направлены на поиск и построение точек в $J_f(\mathbb{Q})$ неизвестных ранее конкретных порядков. Начиная с 1990 года рядом математиков (Flynn, Leprevost, Howe, Poonen, Ogawa, Elkies и другими) было доказано существование \mathbb{Q} -точек кручения якобианов гиперэллиптических кривых рода 2, определенных над \mathbb{Q} , следующих порядков: 11, 13, 15, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 32, 34, 35, 39, 40, 45, 60, 63 (см. [1] и указанную там литературу). Последние найденные \mathbb{Q} -точки кручения датированы 2000 годом.

В серии работ 2009–2010 гг. [2–4] В.П. Платоновым (совместно с В.В. Беньяш-Кривецом) была обнаружена глубокая связь между проблемой существования нетривиальных единиц в гиперэллиптических полях с произвольным полем констант, формальными рядами Лорана, ганкелевыми матрицами, непрерывными дробями и проблемой кручения в якобианах. В 2012 г. в работах [5] и [6] В.П. Платонову (совместно с М.М. Петруниным) с помощью новых эффективных алгоритмов и супервычислений удалось завершить доказательство гипотезы Пунена 1996 г. о существовании \mathbb{Q} -точек любого порядка ≤ 30 в J_f для подходящих f , доказать существование \mathbb{Q} -точек порядков 33, 36 и 48, а также единообразно получить точки кручения всех простых порядков вплоть до 29-го в J_f для подходящих f . В декабре 2012 г. Е. Howe указал якобиан, содержащий \mathbb{Q} -точку кручения 70-го порядка (см. [1]).

В данной статье описан подход к организации супервычислений, связанных с указанным методом Платонова поиска и построения фундаментальных единиц в гиперэллиптических полях с \mathbb{Q} в качестве поля констант. Эти вычисления позволили доказать гипотезу Пунена, а также существование \mathbb{Q} -точек кручения новых порядков, упомянутых выше.

Математические аспекты проблемы

Для дальнейшего изложения необходимо вспомнить несколько понятий и фактов (см. [1]).
Обозначим

$$D_f = \mathbb{Q}[x](\sqrt{f}) = \{\alpha + \beta\sqrt{f} \mid \alpha, \beta \in \mathbb{Q}[x]\}.$$

Элемент $u \in D_f$ называется единицей, если u обратим в кольце D_f . Степень единицы $u = \alpha + \beta\sqrt{f}$ определяется как степень многочлена $\alpha(x)$. Если $u \in \mathbb{Q}^*$, тогда u называется тривиальной единицей в D_f . Предположим, что D_f обладает нетривиальными единицами. Тогда мультипликативная группа $D_f^* = \mathbb{Q}^* \times \langle u_1 \rangle$, где $\langle u_1 \rangle$ – бесконечная циклическая группа. Элемент u_1 называется фундаментальной единицей в D_f .

В работе [3] отмечено, что существование фундаментальной единицы степени m в кольце D_f влечет за собой существование точки кручения степени m в группе $J_f(\mathbb{Q})$. Этот факт позволяет сосредоточиться на поиске фундаментальных единиц колец D_f , так как наличия фундаментальной единицы такого кольца достаточно для существования \mathbb{Q} -точки кручения якобиана J_f соответствующего порядка.

В работе [4] был доказан критерий существования нетривиальных единиц и предложен алгоритм вычисления фундаментальных единиц над любым полем K , характеристика которого отлична от 2. В случае $K = \mathbb{Q}$ критерий выглядит следующим образом.

Без ограничения общности положим $a_6 = 1$ и разложим \sqrt{f} в ряд Лорана:

$$\sqrt{f} = x^3 + d_2x^2 + d_1x + \dots + d_{-k}x^{-k} + \dots.$$

Рассмотрим матрицу

$$H_r = \begin{pmatrix} d_{-1} & d_{-2} & \dots & d_{-r} \\ d_{-2} & d_{-3} & \dots & d_{-r-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{-r-1} & d_{-r-2} & \dots & d_{-2r} \end{pmatrix}.$$

Кольцо D_f имеет нетривиальную единицу $u = \alpha + \beta\sqrt{f}$, где $\alpha, \beta \in \mathbb{Q}[x]$ и $\deg \beta = r$ тогда и только тогда, когда ранг матрицы H_{r+1} меньше, чем $r + 1$, и $\text{rank} H_m = m$ при $m < r + 1$; при этом $\deg u = r + 3$.

Чтобы получить целостное представление об алгоритме, опишем в общих чертах этапы проверки наличия фундаментальной единицы в кольце D_f степени, не более заданной:

- вычислить достаточное количество коэффициентов разложения \sqrt{f} в ряд Лорана;
- вычислять ранг соответствующей матрицы H_r , начиная с $r = 1$ и до тех пор, пока ранг H_r впервые не станет меньше r ; в этом случае в кольце D_f существует нетривиальная единица;
- если же $\text{rank} H_r = r$ для всех r , меньших пороговой величины, то фундаментальной единицы степени, не более заданной, в кольце D_f не существует.

Следующий метод поиска фундаментальных единиц в гиперэллиптических полях имеет другую природу и опирается на результаты теории непрерывных дробей.

Пусть

$$\beta = \sum_{i=s}^{\infty} d_{-i}x^{-i},$$

где β – элемент поля формальных степенных рядов с коэффициентами из \mathbb{Q} .

Положим

$$[\beta] = \begin{cases} \sum_{i=s}^0 d_{-i}x^{-i} = d_{-s}x^{-s} + \dots + d_1x + d_0, & \text{если } s \leq 0 \\ 0, & \text{если } s > 0 \end{cases}$$

Пусть $a_0 = [\beta]$. Если $\beta - a_0 \neq 0$, положим

$$\beta_1 = \frac{1}{\beta - a_0}, \quad a_1 = [\beta_1].$$

Далее по индукции определяем элементы a_i, β_i : если $\beta_{i-1} - a_{i-1} \neq 0$, то

$$\beta_i = \frac{1}{\beta_{i-1} - a_{i-1}}, \quad a_i = [\beta_i].$$

В результате получим непрерывную дробь

$$\beta = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

Можно доказать, что кольцо D_f обладает нетривиальными единицами тогда и только тогда, когда \sqrt{f} разлагается в периодическую непрерывную дробь.

Определим по индукции элементы $p_i, q_i \in \mathbb{Q}[x]$. Положим

$$p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$$

и, если $n \geq 0$, то

$$p_n = a_n p_{n-1} + p_{n-2}, q_n = a_n q_{n-1} + q_{n-2}.$$

Положим

$$A_n = (-1)^{n+1} (p_n^2 - f q_n^2),$$

$$B_n = (-1)^n (p_n p_{n-1} - f q_n q_{n-1}).$$

Видим, что, если существуют такие $i, j, i < j$, что $A_i = A_j, B_i = B_j$, тогда β разлагается в периодическую непрерывную дробь. Таким образом, учитывая вышесказанное, для доказательства наличия в кольце D_f нетривиальной единицы достаточно найти такие номера $i, j, i < j$, что для соответствующих A_i, A_j, B_i, B_j , полученных из разложения \sqrt{f} в непрерывную дробь, выполняется соотношение $A_i = A_j, B_i = B_j$.

Сформулируем в общих чертах второй алгоритм проверки кольца D_f на наличие нетривиальных единиц степени, не более заданной:

- вычислить достаточное количество коэффициентов разложения \sqrt{f} в ряд Лорана;
- вычислить A_i, B_i для соответствующего i ;
- если найдены такие $i, j, i \neq j$, что $A_i = A_j, B_i = B_j$, в кольце D_f существует нетривиальная единица;
- если при достижении индексом i пороговой величины все пары A_j, B_j при $i < j$ различны, фундаментальной единицы степени, не более заданной, в кольце D_f не существует.

Подробно вышеописанные методы и алгоритмы рассмотрены в работах [1–4].

Вычислительные аспекты проблемы

В подходах, предшествующих подходу Платонова, построение точек конечного порядка над полем рациональных чисел на якобианах гиперэллиптических кривых базировалось на исследовании кривых специального вида, таких как модулярные кривые, либо было основано на процедуре, использующей идеи Серра. Во втором случае получающийся в итоге якобиан оказывался изогенным произведению двух эллиптических кривых. Подход к построению якобиана и вычислению соответствующих точек кручения в нем не был унифицирован и требовал отдельных трудоемких вычислений в каждом конкретном случае.

Помимо этого, в системе компьютерной алгебры Magma реализован алгоритм вычисления группы кручения якобиана заданной кривой, что позволяет осуществить перебор подходящих кривых на предмет наличия нетривиальных \mathbb{Q} -точек кручения соответствующих якобианов. Названная реализация достаточно громоздка, и скорость перебора составляет около 320 кривых в секунду при задействовании всех ядер двух процессоров Intel Xeon E5-2670.

Реализация в системе компьютерной алгебры Sage матричной версии алгоритма поиска и построения фундаментальных единиц в кольце D_f и, как следствие, поиска точек кручения позволяет достичь скорости перебора около 640 кривых в секунду на тех же процессорах. Отметим, что реализация в системе Sage версии алгоритма, основанной на использовании непрерывных дробей, а также реализация обеих версий алгоритма на языке C с использованием библиотеки GMP для обеспечения поддержки вычислений над полем \mathbb{Q} не дали существенного прироста производительности по сравнению с реализацией матричной версии алгоритма в системе Sage.

К сожалению, прямой перебор многочленов как в системе Magma (прямое вычисление групп кручения), так и с помощью программных реализаций описанных выше алгоритмов (поиск фундаментальных единиц соответствующих гиперэллиптических полей) над полем рациональных чисел \mathbb{Q} недостаточно эффективен, быстро упирается в вычислительный потолок и не позволяет получать точки кручения новых порядков. Существенная причина невысокой производительности заключается в использовании поля рациональных чисел. Помимо того, что выполнение арифметических операций над полем рациональных чисел сложнее выполнения целочисленных арифметических операций, в ходе работы алгоритма у коэффициентов возникают большие значения числителей и знаменателей, размер которых позволяет разместить их только в нескольких ячейках памяти, что также существенно снижает скорость исполнения.

В значительной степени уменьшить влияние вышеописанной проблемы возможно путем применения

локально-глобального принципа, доказанного в [3]. Ускорения удается добиться редукцией в поле \mathbb{F}_p для подходящих простых p . В этом случае происходит естественное сведение задачи поиска фундаментальных единиц кольца D_f к задаче поиска фундаментальных единиц кольца $D_{f_p} = \mathbb{F}_p[x](\sqrt{f_p})$, где f_p – многочлен, полученный редукцией f в $\mathbb{F}_p[x]$. Для достаточно малых p при использовании \mathbb{F}_p в качестве базового поля все участвующие в вычислении коэффициенты остаются в пределах одной ячейки памяти и в пределах базовых типов используемых языков, что позволяет получить существенный прирост в скорости исполнения по сравнению с вычислениями над полем рациональных чисел.

Вышесказанное можно проиллюстрировать на следующем примере. Для многочлена $f = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ коэффициент d_{-50} разложения \sqrt{f} в ряд Лорана имеет вид

$$d_{-50} = \frac{12764270766313506230756524181}{5070602400912917605986812821504}.$$

В то же время при редукции в \mathbb{F}_{251} его значение становится следующим:

$$d_{-50 \bmod 251} = 45.$$

В некотором роде редукция в конечное поле позволяет осуществить фильтрацию многочленов, поступающих на вход алгоритма над полем рациональных чисел. На вход алгоритма, работающего над полем \mathbb{Q} , будут поступать только многочлены, соответствующее кольцо D_{f_p} которых обладает фундаментальной единицей нужной степени.

Следующим этапом вычислительного развития описываемого метода стал переход от матричной версии на менее ресурсоемкую версию алгоритма, использующую аппарат непрерывных дробей. Можно показать, что оценка количества операций для поиска фундаментальной единицы кольца D_f для заданного f этой версии алгоритма составляет $O(n)$, где n – искомая степень фундаментальной единицы, с константой не более 135.

Применение вышеописанных идей позволяет создать программную реализацию на языке программирования C и избавиться от недостатков, присущих системам компьютерной алгебры и языкам высокого уровня. Совокупный эффект от перехода к операциям в конечном поле, использования аппарата непрерывных дробей и смены языка программирования – прирост скорости более чем на 3 порядка по сравнению с реализацией на Sage для вычислений над \mathbb{Q} . Для случайного набора кривых время проверки над \mathbb{Q} отфильтрованных над конечным полем многочленов оказывается мало по сравнению со временем работы алгоритма фильтрации над \mathbb{F}_p .

Для ускорения программной реализации алгоритма поиска фундаментальных единиц в гиперэллиптических полях с конечным полем в качестве поля констант использовался ряд методов оптимизации. В частности, существенный вклад внесло кеширование арифметических операций над конечным полем (сложение, умножение, взятие обратного). На первом этапе работы программы вычислялись таблицы значений для каждой арифметической операции, а на последующих этапах использовалось не прямое вычисление, а обращение к соответствующей таблице, что дало около 45 % прироста скорости.

В силу особенностей аппаратной архитектуры графические ускорители обладают рядом ограничений, что существенно усложняет процесс разработки и отладки, а также значительно повышает требования к алгоритму. Среди ключевых достоинств алгоритмов, связанных с методом Платонова, важно отметить отсутствие рекурсий, малый объем хранимой промежуточной информации, а также хорошие оценки их алгоритмической сложности как в матричном варианте, так и в варианте с привлечением техники непрерывных дробей. Применение локально-глобального принципа, редукция в поле \mathbb{F}_p и перечисленные достоинства алгоритма, основанного на использовании аппарата непрерывных дробей, позволили создать параллельную программную реализацию алгоритма, оптимизированную для исполнения в гетерогенных вычислительных системах. Вышеупомянутая реализация основана на открытом стандарте OpenCL и способна исполняться как на центральном процессоре, задействуя все его ядра, так и на графических ускорителях.

В качестве аппаратной платформы, на которой производились вычисления, выступает гибридный вычислительный комплекс, собранный в НИИСИ РАН, в составе которого имеются два процессора Intel Xeon E5-2670 и графический ускоритель AMD Radeon HD 7900 Series. На указанном ускорителе на данной задаче удалось достичь более чем восьмикратного ускорения по сравнению с вычислениями на двух процессорах Intel Xeon E5-2670. Помимо указанного оборудования, в распоряжении также находился процессор AMD Opteron Processor 6176SE. Чтобы у читателя сложилась общая картина производительности разработанного алгоритма на различных платформах, приводится сводная таблица скоростей исполнения. В ней сравниваются четыре реализации: на C без кеширования арифметических операций, запущенная ровно на одном ядре процессора (язык C, б/к, одно ядро), на языке C с использованием всех

оптимизаций, запущенная на всех ядрах процессоров одновременно (язык C, кеш., все ядра), на C без кеширования арифметических операций, запущенная на всех ядрах одновременно (язык C, б/к, все ядра), и реализация на базе OpenCL, выполненная в силу особенностей графических ускорителей без кеширования (OpenCL, б/к). В ячейках указано количество исследованных кривых в секунду.

Скорость вычисления на различных архитектурах

Реализация	Opteron	2×Xeon	Radeon HD7901
	24 ядра	32 ядра	–
Язык C, б/к, одно ядро	30200	26700	–
Язык C, б/к, все ядра	725000	855000	–
Язык C, кеш., все ядра	1050000	1200000	–
OpenCL, б/к	600000	700000	10050000

Используя рассматриваемый вычислительный подход для исследования массива кривых $\{f_j\}$ на наличие фундаментальных единиц определенных степеней в кольцах $\mathbb{Q}[x](\sqrt{f_j})$, можно эффективно применить многоступенчатую программную реализацию. На первых двух этапах для некоторых p производится быстрый предварительный отсев многочленов, соответствующие редуцированные кольца $\mathbb{F}_p[x](\sqrt{f_{p,j}})$ которых не обладают фундаментальными единицами искомым степеней. На третьем, заключительном, этапе значительно уменьшенный на предшествующих этапах массив кривых поступает на вход алгоритма, работающего над \mathbb{Q} , что позволяет на выходе получить искомые кривые из первоначального массива. Правильно подобрав набор простых p_i , можно утверждать, что с высокой вероятностью массив, отфильтрованный с помощью редукций к соответствующим \mathbb{F}_{p_i} , будет полностью состоять из кривых, чьи кольца D_{f_j} будут обладать фундаментальными единицами искомым степеней. Для случайно выбранного массива кривых при правильно подобранных p_i время исполнения последнего этапа пренебрежимо мало по сравнению со временем исполнения первых двух этапов, когда вычисления осуществляются над полями F_{p_i} .

Описанная многоступенчатая реализация также была разработана с использованием стандарта OpenCL для вышеуказанного вычислительного комплекса, причем удалось одновременно задействовать как центральные процессоры, так и графические ускорители.

Более подробно опишем первые два этапа. Напомним, что для произвольного многочлена 6-й степени $f_p(x) \in \mathbb{F}_p[x]$, свободного от квадратов, соответствующее кольцо $D_{f_p} = \mathbb{F}_p[x](\sqrt{f_p(x)})$ всегда обладает нетривиальными единицами. Основного ускорения удается достичь за счет предварительного вычисления фундаментальных единиц ограниченной степени всех многочленов 6-й степени в $\mathbb{F}_{p_i}[x]$ для малых простых p_i . Вычисленные единицы помещались в соответствующие таблицы и сохранялись на жестком диске.

Очевидно, что всякому многочлену $f_{\mathbb{Q}} \in \mathbb{Q}$, соответствующее кольцо $D_{f_{\mathbb{Q}}}$ которого обладает фундаментальной единицей степени n , можно сопоставить многочлен $f_{\mathbb{Z}} \in \mathbb{Z}$, соответствующее кольцо $D_{f_{\mathbb{Z}}}$ которого обладает фундаментальной единицей степени n . На первом этапе для каждого многочлена $f_p \in \mathbb{F}_p[x]$, соответствующее кольцо D_{f_p} которого обладало фундаментальной единицей заданной степени, вычислялись все многочлены $f \in \mathbb{Z}[x]$, коэффициенты которых попадали в определенный диапазон и при этом совпадали с соответствующими коэффициентами f_p при редукции в поле \mathbb{F}_p . Далее, на втором этапе, эти многочлены редуцировались по нескольким различным простым p_j и отсеивались те многочлены, соответствующие редуцированные кольца $\mathbb{F}_{p_j}[x](\sqrt{f_{p_j}})$ которых не обладают фундаментальными единицами искомым степеней. Для получения дополнительного ускорения отсеивание также происходило путем сопоставления редуцированного многочлена и заранее вычисленной степени единицы, сохраненной в таблице.

Используя свойства гиперэллиптических кривых, удается сократить количество многочленов в $F_p[x]$,

в соответствующих кольцах которых вычисляются фундаментальные единицы. Как следствие, без ограничения общности удастся уменьшить количество предварительно найденных многочленов, что позволяет, с одной стороны, сократить перебор, а с другой – увеличить простые p , для которых составляются упомянутые выше таблицы, что гарантирует дополнительное ускорение. Так, увеличение на предварительном этапе простого p в два раза влечет четырехкратное ускорение нахождения всех фундаментальных единиц ограниченной степени колец $D_f = \mathbb{Q}[x](\sqrt{f(x)})$ для $f \in \mathbb{Z}[x]$, коэффициенты которых ограничены константой C .

За счет оптимизаций на всех трех этапах выполнения удалось достичь скорости исполнения, более чем на четыре порядка превышающей скорость выполнения упомянутой ранее одноступенчатой OpenCL-реализации.

Таким образом, в результате перехода к алгоритму, использующему аппарат непрерывных дробей, многоступенчатой фильтрации путем редукции в соответствующие \mathbb{F}_p и применения многочисленных математических и вычислительных оптимизаций алгоритма удалось достичь скорости перебора кривых более чем на девять порядков выше, чем при использовании реализации над \mathbb{Q} или реализации алгоритма поиска точек кручения на основе системы компьютерной алгебры Magma, что позволило доказать существование точек кручения новых порядков, указанных во введении к настоящей статье.

Автор благодарит сотрудников НИИСИ РАН Малого А.А. и Богданова П.Б. за консультации и помощь, оказанную в процессе разработки программных реализаций, описанных в настоящей статье.

Литература

1. Платонов В.П. Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // Успехи матем. наук. 2014. Т. 69. № 1. С. 3–38.
2. Беляш-Кривец В.В., Платонов В.П. Группы S-единиц в гиперэллиптических полях и непрерывные дроби // Математический сборник. 2009. Т. 200. № 11. С. 15–44.
3. Платонов В.П. Арифметика квадратичных полей и кручение в якобианах // Доклады РАН. 2010. Т. 430. № 3. С. 318–320.
4. Беляш-Кривец В.В., Платонов В.П. О новом локально-глобальном принципе для квадратичных функциональных полей // Доклады РАН. 2010. Т. 433. № 2. С. 154–157.
5. Платонов В.П., Петрунин М.М. Новые порядки точек кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады РАН. 2012. Т. 443. № 6. С. 664–667.
6. Платонов В.П., Петрунин М.М. О проблеме кручения в якобианах кривых рода 2 над полем рациональных чисел // Доклады РАН. 2012. Т. 446. № 3. С. 263–264.
7. Stein W.A. et al. Sage Mathematics Software. The Sage Development Team. URL: <http://www.sagemath.org> (дата обращения: 1.07.2014).
8. Bosma W., Cannon J. J., Fieker C., Steel A. (eds.). Handbook of Magma functions, Edition 2.16 (2010), 5017 p.
9. Khronos Group, Open Computing Language (OpenCL)/ URL: <https://www.khronos.org/opencv/> (дата обращения: 1.07.2014).