Предарифметика*

И. Кулаков, random-art.ru

Многолетние исследования в области стохастических систем привели к совершенно неожиданному результату. Оказалось, что обычные арифметические действия не столь тривиальны**,** как это безоговорочно принимается. В основе арифметики лежит ***предарифметика***, о чем свидетельствуют приводимые в статье результаты. В отличие от арифметики, предарифметика тривиальна и неразложима на элементарные составляющие. Из предарифметики следуют и другие ее разновидности, а с ними и новые арифметики. По сути, предарифметики знаменуют начало развития ***новой***, ***обладающей уникальными свойствами алгебраической базы*** по форме, содержанию и достигаемым результатам кардинально отличающейся от всех других известных на сегодня аналогов.

В двоичной арифметике результат сложения $g = a + b$, двух n-разрядных двоичных величин $\{a,b\}$, может быть задан ***исходя не из привычных правил позиционного счета*** [1], а из правил, когда результат операции определяется не одним, а ***всеми признаками переноса одновременно*** [2].

Быстрое сложение и вычитание в арифметике

В первую очередь, из правил позиционного счета следует, что операция сложения по всем признакам переноса может быть осуществлена исходя из следующего уравнения:

$$g = a + b = 2\cdot(a \,\&\, b) + (a \oplus b). \qquad (1)$$

Знаками & и ⊕ обозначены двоичные операции **И**, **ИСКЛЮЧАЮЩЕЕ ИЛИ** (**XOR**) – сложение по модулю 2, над n-разрядными двоичными величинами.

В свою очередь, операция сложения (1) допускает рекурсивное разложение в последовательность элементарных действий, через введение промежуточной двоичной переменной $\boldsymbol{p}$. Для этого первоначально положим $g_0 = a$ и $p_0 = b$. Тогда из соотношения (1) следует, что

$$g_1 = g_0 \oplus p_0, \qquad p_1 = 2\cdot(g_0 \,\&\, p_0), \qquad \text{при этом} \qquad g_1 + p_1 \bmod 2^n = a + b,$$

а двоичная переменная p, содержит все признаки переноса, формируемые по всем n двоичным разрядам, одновременно.

Далее, по индукции, на втором и каждом последующем k-ом шаге, имеем:

$$g_2 = g_1 \oplus p_1, \qquad p_2 = 2\cdot(g_1 \,\&\, p_1), \qquad \text{при этом} \qquad g_2 + p_2 \bmod 2^n = a + b;$$

. . . . . .

$$g_k = g_{k-1} \oplus p_{k-1}, \qquad p_k = 2\cdot(g_{k-1} \,\&\, p_{k-1}), \qquad \text{при этом} \qquad g_k + p_k \bmod 2^n = a + b;$$

При $p_k \bmod 2^n = 0$ $(k \le n)$, когда все признаки переноса p становятся нулевыми, имеем, что $g_k + 0 = a + b$, т. е. двоичная переменная g становится равной сумме двух, связанных двоичной операцией сложения величин.

Таким образом, из соотношения (1) следует формальное разложение операции сложения $g = a + b$ в последовательность $\boldsymbol{k}$ простейших, *равноустроенных и не выводимых* друг из друга элементарных, параллельно исполняемых действий над двоичными разрядами числовой пары $\{g, p\}$ – результатом операции g и его n-разрядным ***нелинейным дополнением*** $\boldsymbol{p}$, ***образованным всеми признаками переноса***. А именно, разложение, подчиняющееся следующим рекурсивным уравнениям:

$$p_k = (g_{k-1} \,\&\, p_{k-1}) \lessdot 1 \qquad (p_{k-1} \neq 0), \qquad g_k = g_{k-1} \oplus p_{k-1} \qquad (2)$$

со смещением $\lessdot 1$ на один разряд в сторону старших значащих бит, при начальных условиях $p_0 = b$ и $g_0 = a$. По ходу рекурсии через $\boldsymbol{k \le n}$ шагов дополнение $p = 0$ обращается в ноль, свой-

ственный ординарной (классической) арифметике – $a + b = g$. При этом операция сложения, представляемая рекурсивным уравнениям (2), выполняется намного быстрее, чем это мы делаем посредством обычных правил позиционного счета.

Пример выполнения операции сложения двух 32-х разрядных двоичных чисел по всем признакам переноса одновременно, показан на рис.1.

операция сложения $g = g_0 + p_0 \ mod\ 2^{32}$									**результат**
p_0	1010	0111	1001	1101	0100	1101	0100	1011	**2812104011**
g_0	1110	1001	1100	0110	0001	1001	0101	0111	**3922073943**
p_1	1 0100	0011	0000	1000	0001	0010	1000	0110	5419569798
g_1	0 0100	1110	0101	1011	0101	0100	0001	1100	1314608156
p_2	0 1000	0100	0001	0000	0010	0000	0000	1000	2215649288
g_2	1 0000	1101	0101	0011	0100	0110	1001	1010	4518528666
p_3	0 0000	1000	0010	0000	0000	0000	0001	0000	136314896
g_3	1 1000	1001	0100	0011	0110	0110	1001	0010	6597863058
p_4	0 0001	0000	0000	0000	0000	0000	0010	0000	268435488
g_4	1 1000	0001	0110	0011	0110	0110	1000	0010	6465742466
p_5	0 0000	0000	0000	0000	0000	0000	0000	0000	0
g_5	**1** 1000	1101	0101	0011	0110	0110	1001	1010	**6734177954**

Рис. 1

Аналогично, через двойное отрицание $d = \overline{\overline{a} + b}$ согласно выражениям:

$$p_k = (\overline{d}_{k-1} \,\&\, p_{k-1}) \lessdot 1 \quad (p_{k-1} \neq 0), \qquad d_k = d_{k-1} \oplus p_{k-1}, \tag{3}$$

при начальных условиях $p_0 = b$ и $d_0 = a$, посредством инверсии **НЕ**, обозначаемой знаком $\overline{\ }$, может быть вычислена разность $d = a - b$ двух величин.

Пример выполнения операции вычитания двух, используемых в примере сложения, чисел по всем признакам переноса одновременно, показан на рис.2.

операция вычитания $g = d_0 - p_0 \ mod\ 2^{32}$									**результат**
p_0	1010	0111	1001	1101	0100	1101	0100	1011	**2812104011**
d_0	1110	1001	1100	0110	0001	1001	0101	0111	**3922073943**
	0001	0110	0011	1001	1110	0110	1010	1000	$\overline{d}_0$
p_1	0000	1100	0011	0010	1000	1000	0001	0000	204638224
d_1	0100	1110	0101	1011	0101	0100	0001	1100	1314608156
	1011	0001	1010	0100	1010	1011	1110	0011	$\overline{d}_1$
p_2	0000	0000	0100	0001	0001	0000	0000	0000	4263936
d_2	0100	0010	0110	1001	1101	1100	0000	1100	1114233868
p_3	0000	0000	0000	0000	0000	0000	0000	0000	0
d_3	0100	0010	0010	1000	1100	1100	0000	1100	**1109969932**

Рис. 2

Неполная арифметика и предарифметика

При ограничении общего числа шагов $k \leq \delta$, иначе ***глубины переноса*** $\delta < n$ в выражениях (2) и (3), операции сложения и вычитания, как и следующая из них арифметика неполна. Неполная арифметика с минимальной глубиной переноса ($\delta = 1$), не далее чем на разряд, получила название – ***предарифметика***.

Предарифметика и операции в ней

Сложение* (*вычитание*) *в предарифметике, как следует из соотношений (2) и (3) подчиняется ряду, формируемому согласно с уравнениями:

$$P_i = ((\boldsymbol{Imp}(G_{i-1}) \,\&\, P_{i-1}) \lessdot_1) \mid \mathbf{1}, \qquad G_i = G_{i-1} \oplus P_{i-1} \ mod\, 2^n \tag{4}$$

с функцией импликации $\boldsymbol{Imp}(c) = c$ для сложения и $\boldsymbol{Imp}(c) = \overline{c}$ для вычитания, включающим две двоичные переменные $\{G,P\}$ – n-разрядную базу операции G и ее $(n+1)$-разрядное нелинейное дополнение P, путем прибавления (вычитания) единицы **1**, фиксируемой в младшем разряде дополнения P, начиная с начальных значений $\{G_O,P_O\}$.

На рис.3 и рис.4 приведены ряды, полученные при нулевых начальных условиях $P_O = 0$ и $G_O = 0$, составленные из упорядоченных пар (G_i,P_i), *представляющих собой бинарные отношения*, задающие операцию сложения и вычитания в предарифметике, и результаты операций сложения g с единицей и ее вычитания d в 4-х разрядной двоичной арифметике.

По отношению к предарифметике и арифметике, может быть введена и двойственная по отношению к ним комплементарная предарифметика и арифметика.

Сложение* (*вычитание*) *в комплементарной предарифметике подчиняется ряду, следующему из соотношений (4) и комплементарного свойства $a \mid b = \overline{\overline{a} \,\&\, \overline{b}}$, формируемому при $P' = \overline{P}$ и $G' = \overline{G}$, согласно с уравнениями:

$$P'_i = (\boldsymbol{Imp}(G'_{i-1}) \mid P'_{i-1}) \lessdot_1, \qquad G'_i = \overline{G'_{i-1} \oplus P'_{i-1}} \ mod\, 2^n, \tag{5}$$

начиная с начальных значений $\{P'_O,G'_O\}$.

На рис.5 и рис.6 приведены ряды, полученные при нулевых начальных условиях $P'_O = 0$ и $G'_O = 0$, составленные из упорядоченных пар (G'_i,P'_i), задающих операцию сложения и вычитания в комплементарной предарифметике, и результаты операций сложения g' с единицей и ее вычитания d' в 4-х разрядной комплементарной арифметике.

Нелинейное дополнение арифметических действий

По определениям (2) - (5) в неполной арифметике и предарифметике ***дополнение p составляет неотъемлемую часть операций***, ***не имеет самостоятельного назначения***, ***носит строго выраженный нелинейный характер***, ***не вырождается в константу и не исчезает***, как это имеет место в следующих из них ординарной и комплементарной ей арифметике, при глубине переноса $\boldsymbol{\delta = n}$, равной $\boldsymbol{n}$ разрядности чисел.

Нестационарные процессы и саморегуляция

В приведенных двух предарифметиках, задаваемых уравнениями (4) и (5), в отличие от арифметик, возможно наличие зависящего от начальных условий переходного нелинейного участка, длиной $L_T \le n$, после прохождения которого базовая переменная G, ***благодаря феноменальной саморегуляции*** ее и ее ***нелинейного дополнения*** P, ***достигает максимального периода*** 2^n и далее всюду, в границах каждого из последующих периодов ***ведет себя стационарно и бесповторно*** (***апериодично***), что демонстрируется на рис.3 - рис.6.

Наличие такого нестационарного переходного участка (аттрактора), самоисчезающего по мере формирования последующих элементов последовательностей, задаваемых уравнениями (4) и (5), существенно отличается от подобных участков (предпериодов), наблюдаемых при генерации периодических последовательностей на основе рекуррентных подходов [3], а также поведением на этих участках, как правило, ведущим к трудно предсказуемому, нестабильному поведению генераторов, а в особых случаях и к их полному вырождению.

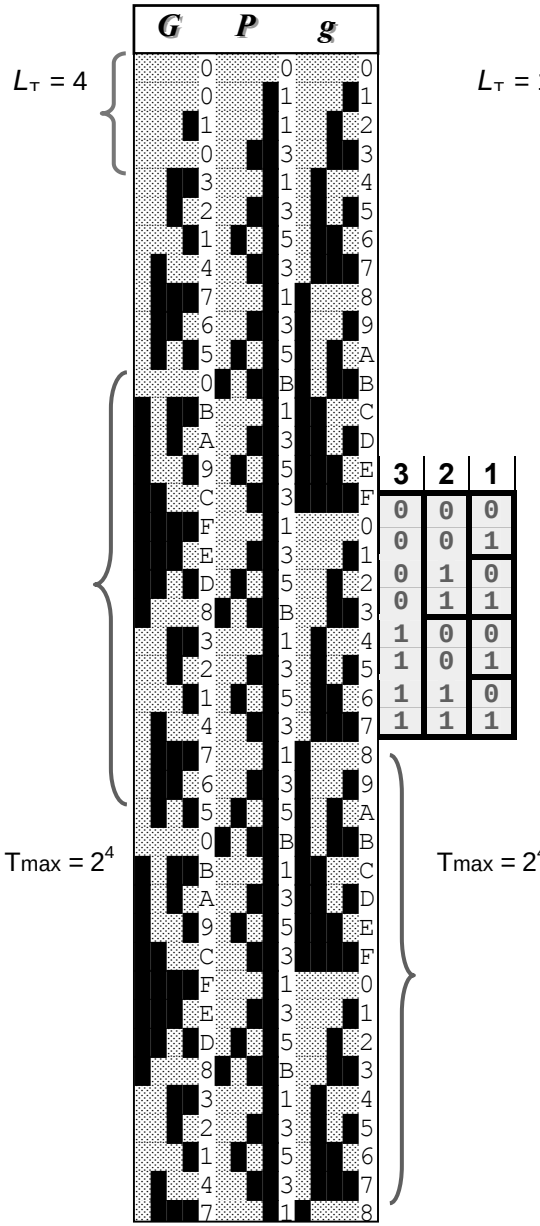

Рис. 3

3	2	1
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

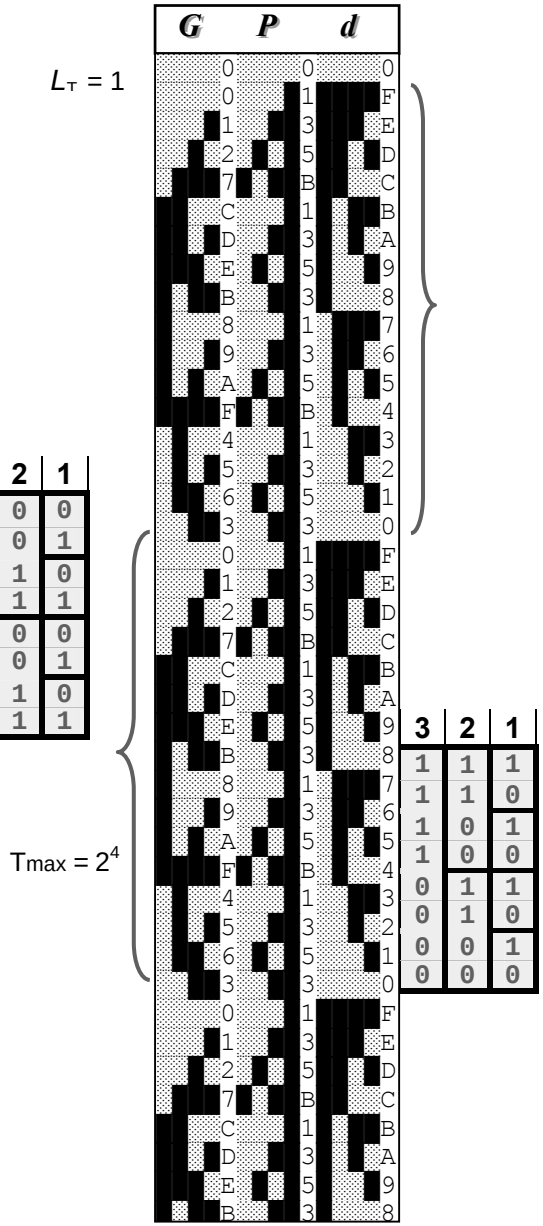

Рис. 4

3	2	1
1	1	1
1	1	0
1	0	1
1	0	0
0	1	1
0	1	0
0	0	1
0	0	0

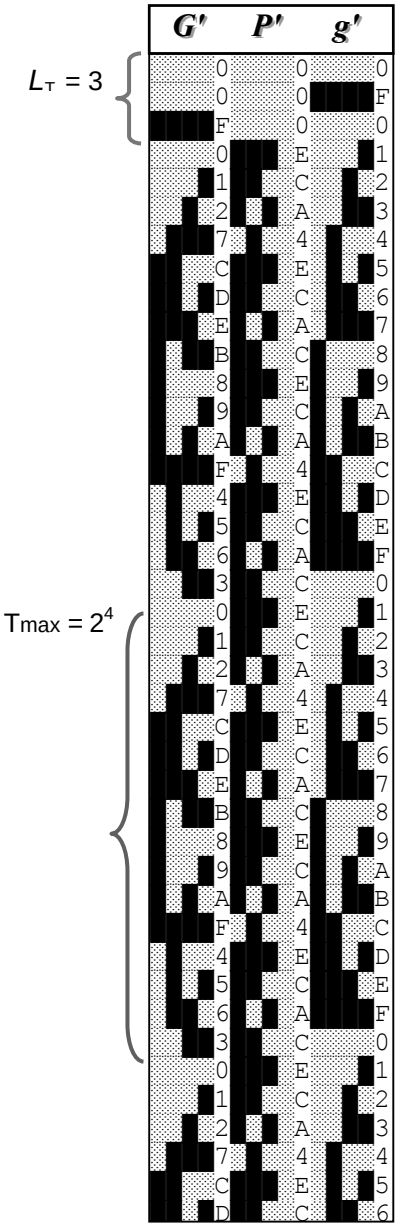

Рис. 5

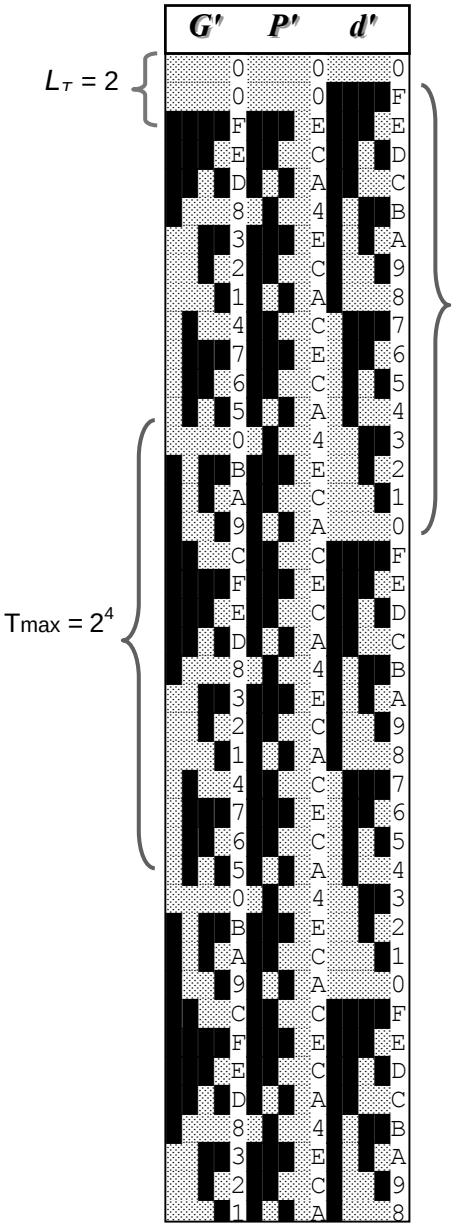

Рис. 6

Вместе с тем, число таких разнообразных последовательностей равно 2^n, а не 2^{2n}, как можно было бы ожидать исходя из всего разнообразия начальных условий $\{G_O,P_O\}$, и по существу определяется исходя из всевозможных значений начального элемента $G_{iO}\in\{G_i\}$ и строго приданного ему элемента $P_{iO}\in\{P_i\}$. Иными словами, упомянутый выше ***процесс саморегуляции*** не дается бесплатно и ***приводит к строгой взаимозависимости базы G и ее дополнения P***.

Заключение

Открытие предарифметики и неполной арифметики, предшествующих обычной, классической арифметике, а также следующих из нее разновидностей, как видится по материалам проведенных исследований (**random-art.ru**), знаменует начало развития ***новой алгебраической базы***, по своим потенциальным и функциональным возможностям, и главное, по первооснове, эффективности и качеству результатов реализации, заметно превосходящей все известные рекуррентные [3] и стохастические методы обработки, в том числе и в полях Галуа [4].

Собственно, все результаты, вопреки скоропалительному сарказму и не подкрепленному фактами недоверию к представленным результатам, подтверждаются на детально выверенных моделях разработанных автором [5], а также независимыми исследованиями [6] и экспертизой [7], которые могут быть легко воспроизведены, не только владеющими основами программирования начинающими учеными и специалистами среднего профиля, но и творческой молодежью и продвинутыми школьниками.

Самые последние идеи и результаты, закладывающие теоретическую и раскрывающие прикладную основу предарифметики и ее разновидностей, а также следующей из них алгебраической базы, отражены в статье «**Гипотеза о природе Арифметики**» (**random-art.ru**).

В целом, опираясь на результаты многолетних исследований и разработок, введение предарифметики и следующей из нее алгебраической базы, как видится, позволит обогатить теорию чисел, физику и математику, а с ними осуществить качественный скачек в развитии теории динамических и стохастических систем, теории Хаоса и представляемых ими методов и технологий цифровой обработки.

1. Кнут Дональд Э. Искуство программирования,
   Третье издание, Том 1-2, М.: Издательский дом “Вильямс”, 2002.
2. Weller C. W. High-Speed Carry Ckt. For Binary Adders.
   IEEE Trans. On Computers vol. C-18, No.8, Aug. 1969, pp. 728-732.
3. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра.
   М.: Гелиос АРВ, 2003.
4. Иванов М.А. Криптографические методы защиты информации в компьютерных
   системах и сетях. КУДИЦ-ОБРАЗ, Москва 2001.
5. Кулаков И.А. Стохастические системы и криптография.
   Материалы конференции РусКрипто 2006, Москва, февраль 2006.
6. Тун Мья Аунг. Разработка и исследование стохастических методов защиты программных
   систем. Диссертация на соискание ученой степени кандидата технических наук:
   05.13.11, 05.13.19, Москва, 2007 198 с. РГБ ОД, 61:07-5/2492.
7. Иванов А.Г. Анализ алгоритма односторонней аутентификации.
   Материалы НИР «Система контроля сертификационных меток» и ее экспертизы,
   Московский комитет по науке и технологиям, Москва, 2005-2006, **random-art.ru**.
