

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
имени М.В. ЛОМОНОСОВА**

---

**НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ  
ЯДЕРНОЙ ФИЗИКИ имени Д.В. СКОБЕЛЬЦЫНА**

Басиладзе С.Г.

**Виртуальные состояния  
как следствие информационных ограничений,  
вычисления на основе виртуальных состояний**

Препринт НИИЯФ МГУ № 2011-3/867

Москва, 2011 г.

УДК 519.72 + 539.12  
PACS 29.40 + 03.67

С.Г.Басиладзе

e-mail : [Sergey.Basiladze@cern.ch](mailto:Sergey.Basiladze@cern.ch)

## **Виртуальные состояния как следствие информационных ограничений, вычисления на основе виртуальных состояний**

Препринт НИИЯФ МГУ №

Аннотация

Из-за наличия шумов и ограничения скорости реального сигнала принципиально не может быть четких ступенчатых границ между соседними состояниями, т.е. должны существовать переходные зоны, где оба состояния существуют как бы одновременно.

Перекрытие границ вблизи порога восприятия порождает виртуальные (подпороговые) состояния. Их существование выглядит как неопределенность, выражающаяся в наличии случайных отклонений от распознаваемых состояний к их соседям в многомерном логическом пространстве.

Рассмотрены возможности и ограничения использования виртуальных состояний для проведения сверхбыстрых вычислений.

**S.G.Basiladze**

## **Virtual states as consequence of information restrictions, calculations on the basis of virtual states**

Preprint MSU SINP №

Abstract

Because of noise and basic restriction of speed of a real signal, there cannot be accurate step borders between the adjacent states, i.e. there should be transitive zones where both states exist as though simultaneously.

Overlapping of borders near to a perception threshold generates virtual (under threshold) states. Their existence looks as an uncertainty expressed available of casual deviations from distinguished states to their neighbors in multidimensional logical space.

Possibilities and limitations of use of virtual states for carrying out of superfast calculations are considered.

## Введение

Настоящая работа посвящена анализу возможных форм существования состояний сигналов, находящихся на уровне или ниже порога восприятия и отображающих явления реального мира. Работа является продолжением [1], где рассматривались различия между сигналом, соответствующим подходам классического математического анализа (использование бесконечно малых и допущение бесконечно больших величин) и реальным сигналом, принципиально имеющим [2,3] пороговое и предельное информационные ограничения.

Информационный порог порождается конечностью энергии, требуемой для восприятия сигнала, к чему может добавляться и конечность быстроты процесса восприятия. Наличие информационного порога является физической основой существования дискретных – различимых состояний реального сигнала [4]. Главным, обсуждаемым в данной работе, является вопрос о том, насколько четко различаются соседние состояния сигнала при наличии информационного порога. При пороге только по энергии, границы между состояниями, которые, теоретически, могут быть ступенчатыми, размываются из-за наличия шумов. При дополнительном ограничении по скорости – когда появляется порог по действию и классический шум пропадает (он интегрируется [3]), все равно, принципиально не может быть резких ступенчатых границ между состояниями [4].

Если сигнал находится вблизи порога восприятия, то перекрытие границ порождает так называемые виртуальные (подпороговые) состояния. Их необычность состоит в том, что они проявляются как неопределенность, состоящая в наличии шумовых - случайных отклонений от классических состояний к их соседям в логическом пространстве.

Рассмотрены возможности и ограничения использования виртуальных состояний для проведения быстрых вычислений там, где решение достигается нахождением максимума или периода функции.

В данной работе приняты следующие правила выделения слов: наиболее важные - ключевые слова и фразы подчеркиваются. Вводимые по ходу изложения термины записываются курсивом и подчеркиваются; далее термины могут выделяться курсивом для уведомления, что в данном месте это слово понимается только в узко определенном значении.

## Сигнал и его состояния

**Два вида восприятия сигнала.** В физике широко используется понятие потенциала – рис.1,а, как общее, отвлеченное от конкретных механизмов действия, средство для описания процессов и явлений, сопровождающихся изменениями энергии. При таком подходе сигнал – рис.1,б является производной от потенциала по координате или по времени [3,4]. Процесс восприятия (распознавания) сигнала всегда инерционен и связан с некоторой постоянной времени регистрации  $\tau_R$  (рис.1,в,д). Для удобства расчетов можно полагать, что процесс регистрации сигнала идеален и не обладает инерцией, но сам воспринимаемый сигнал является интегрированным (затянутым) с постоянной времени  $\tau_R$  – рис.1,г,е [4].

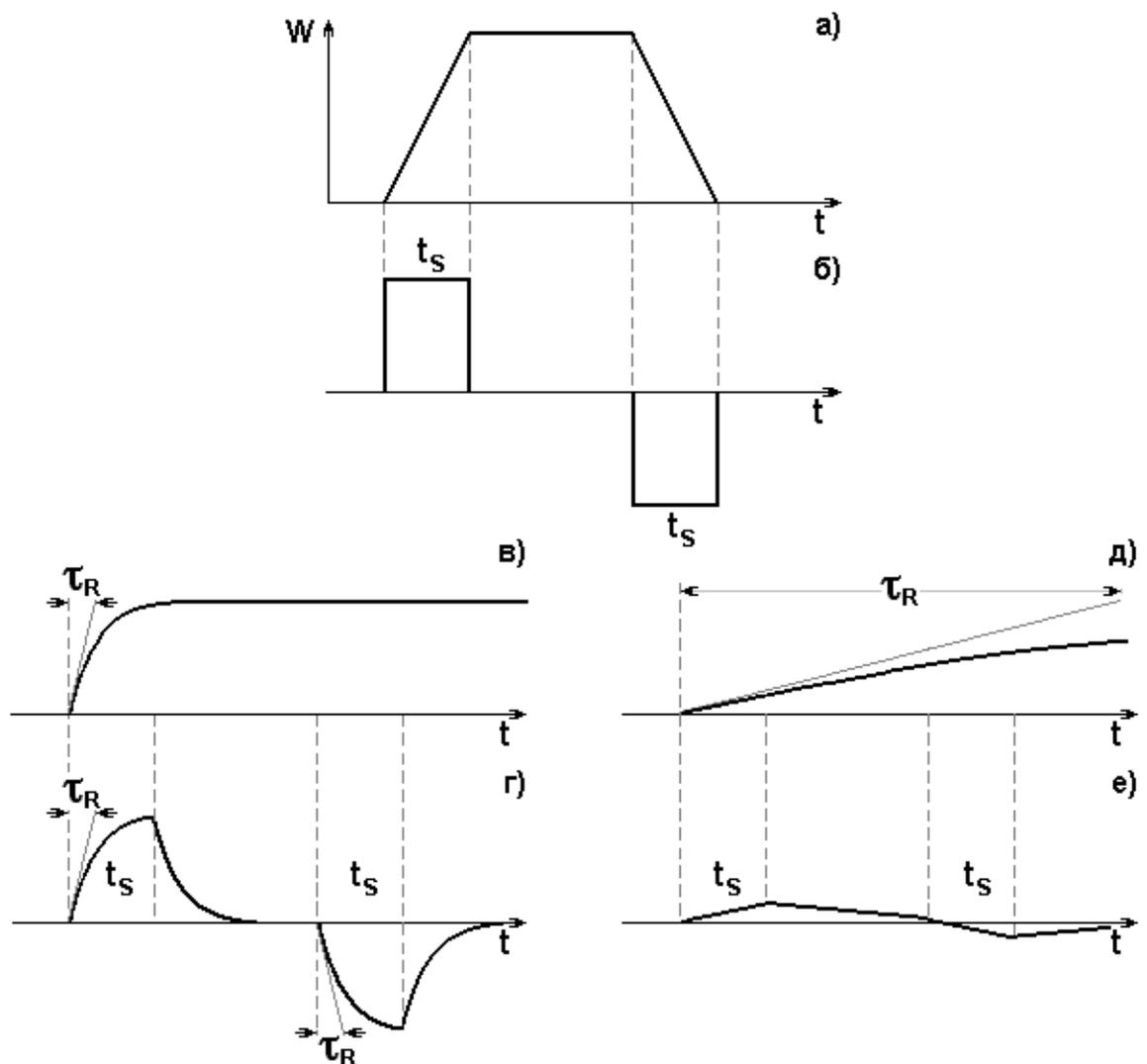


Рис.1. Восприятие сигнала при *быстром* (слева) и *медленном* (справа) процессах регистрации: а) линейная аппроксимация потенциального барьера; б) сигнал как производная от потенциала  $W$ ; в),д) постоянные времени быстрого и медленного процессов регистрации; г),е) воспринимаемые сигналы с учетом инерционности процесса регистрации (интегрированы с постоянной  $\tau_R$ ). Быстрый – незначительно интегрирующий процесс “видит” оба разнополярных сигнала (по отдельности). Медленный процесс, сильно интегрирующий оба сигнала, при наличии порога по действию “не видит” ни одного из них, т.к. их суммарное действие близко к нулю и находится ниже порога. В результате, потенциальный барьер, уверенно воспринимаемый в *быстром* процессе регистрации – г), может быть совсем не воспринимаемым, т.е. прозрачным в *медленном* процессе – е).

Хотя инерционность есть всегда, восприятие может быть быстрым и медленным – в зависимости от отношения  $\tau_R$  к длительности сигнала.

При быстром восприятии (левая колонка на рис.1)  $\tau_R$  пренебрежимо мала. Если же постоянная инерционности механизма восприятия  $\tau_R$  существенно больше, чем длительность сигнала (правая колонка на рис.1), то

а) воспринимаемая часть сигнала, оказывается практически лишенной верхних гармоник – рис.1,е, потому, что сам сигнал почти полностью интегрирован;

б) восприниматься начинает не энергия (исходного) сигнала, а квадрат его площади (напомним, что квадратом площади, т.е. квадратом постоянной составляющей сигнала [2] является действие).

Если же  $\tau_R$  существенно больше еще и расстояния между группой сигналов, то в) они воспринимаются как один сигнал с общим действием (сигналы при этом складываются по площадям, т.к. действие сигнала есть квадрат его площади).

Пункт в) означает, что имеет место алгебраическое сложение (интерференция) огибающих интегрированных сигналов – рис.1,е.

Если, как показано на рис.1,а, потенциальный барьер симметричен, то он порождает два одинаковых разнополярных сигнала, которые при медленном процессе регистрации вообще не воспринимаются (их суммарная площадь на рис.1,е практически нулевая). Однако, при быстром восприятии (на рис.1 слева) каждый из сигналов является “видимым”. Эффект прозрачности такого узкого потенциального барьера является следствием интерференции интегрированных сигналов. Вообще говоря, если интегрирование не совсем полное, то и при медленном процессе регистрации можно добиться восприятия потенциала, значительно повысив величину  $W$ ; однако, эффективность использования энергии  $W$  будет крайне низкой по сравнению с быстрым процессом.

Классический сигнал обычно сопровождается шумом, уровень которого прямо пропорционален ширине полосы частот и, следовательно, он обратно пропорционален  $\tau_R$  (воспринимаемая полоса частот равна:  $\Delta f_R = 1/2\pi\tau_R$ ; более высокие гармоники исчезают при интегрировании, т.к. их площадь нулевая). Это значит, что в правой колонке на рис.1 при  $\tau_R \rightarrow \infty$  классический шум не действует, ибо он не имеет постоянной составляющей в своем спектре.

**Классические комбинационные состояния.** В классической алгебре логики подразумевается ступенчатая – скачкообразная граница между соседними состояниями одного сигнала. При двух (логических) состояниях, выбранное по любому отличительному признаку состояние  $A$  четко отличается от  $\overline{A}$  (не- $A$ ), т.е. от всего остального – рис.2,а. Два независимых признака  $A, B$  (у двух классических сигналов) и их антиподы –  $\overline{A}, \overline{B}$  дают 4 возможных сочетания:  $\overline{B} \overline{A}$  (00),  $\overline{B} A$  (01),  $B \overline{A}$  (10) и  $BA$  (11). Эти сочетания являются производными - комбинационными состояниями (второго ранга или уровня). Их можно представить – рис.2,б картой Карно или Вейча [5], как зоны “ортогонального пересечения” клеток  $\overline{A}, A$  и  $\overline{B}, B$  на плоскости.

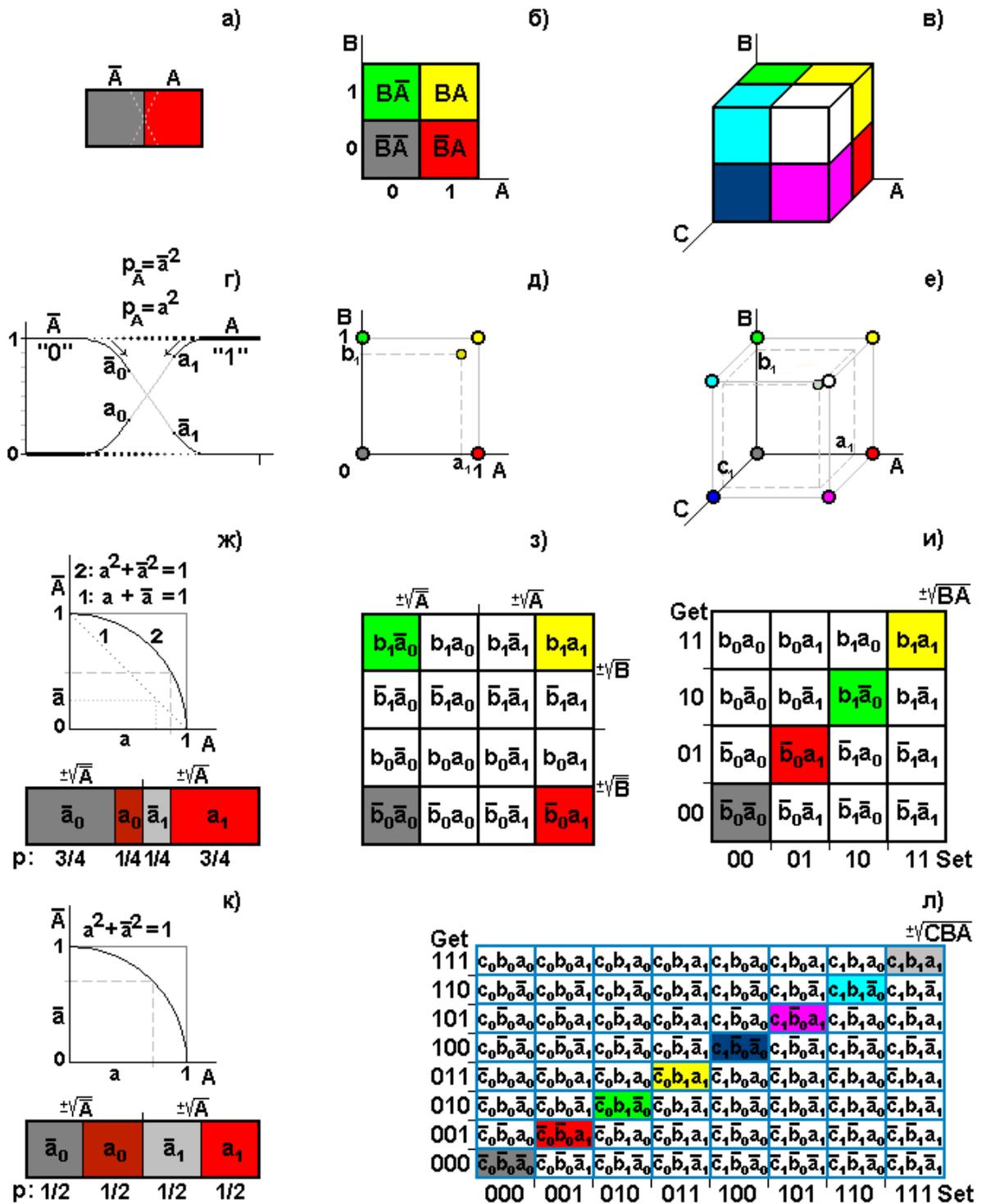


Рис.2,а)÷в) классические абсолютно четко заданные 1-, 2- и 3-мерные состояния; а),г) состояние и его альтернатива, “взаимопроникающие” друг в друга, когда их границы не ступенчатые; д),е) эти же состояния как точки в аналогово-логическом пространстве; ж),к) квадраты наследуемого и альтернативного виртуальных состояний дают вероятности появления соответствующих классических состояний; з),и) карта и таблица двумерных виртуальных состояний; сумма всех произведений вероятностей по каждому столбцу таблиц и) и л) равна единице; наследуемые состояния располагаются по (основной) диагонали.

Чтобы упростить записи в каждой клетке, квадраты величин  $\bar{a}$ ,  $a$ ,  $\bar{b}$ ,  $b$ ,... в ж)÷и) условно показаны в первой степени (в виде радикалов); для напоминания об этом у базовых переменных  $A, B, \dots$  в картах и таблицах поставлен знак корня со знаком '±'.

Три независимых признака  $A$ ,  $B$ ,  $C$  совместно с  $\overline{A}$ ,  $\overline{B}$ ,  $\overline{C}$  дают 8 возможных комбинаций и образуют двоичный куб состояний; на рис.2,в он изображен как куб 3-х основных (рис.2,б) и 4-х переходных цветов, плюс “не-цвет” (на рис.2,а,б он показан темно-серым).

Состояния  $\overline{A}$  и  $A$  можно также показать точками '0' и '1' на отрезке математической оси. Состояния  $A$  и  $B$  – рис.2,д тогда будут располагаться по двум ортогональным осям (они независимы), а  $A$ ,  $B$  и  $C$  – по трем ортогональным координатам (на краях единичных отрезков, рис.2,е); состояние же “полного отсутствия”  $\overline{A} \overline{B} \overline{C}$  (темно-серое) будет общим, оно находится в начале координат.

Все сказанное выше о состояниях, соответствует быстрому процессу регистрации и полному отсутствию шума, т.е. графикам левой части рис.1.

### Комбинационные виртуальные состояния

Реальный сигнал всегда имеет определенный порог восприятия, отражающий тот очевидный факт, что для восприятия сигнала необходима конечная (ненулевая) энергия. Само по себе наличие порога по энергии говорит, скорее, в пользу достаточно четкой границы между состояниями. Однако, присутствие классического шума может существенно размыть границы состояний. Как уже говорилось, среднеквадратичное отклонение классического шума пропорционально ширине полосы частот; оно также пропорционально его характеристической энергии. Для теплового шума это  $4kT$  ( $k$  – постоянная Больцмана,  $T$  – абсолютная температура), а для дробового электрического шума –  $2e \cdot \Delta U$ , где  $e$  – заряд электрона, а  $\Delta U$  – разность потенциалов, проходимая носителями электрических зарядов (здесь и ниже, во избежание смешивания обозначений, физические величины записываются курсивом). Поэтому когда характеристическая энергия шума сопоставима с пороговой энергией, то неизбежно частичное пересечение соседних состояний, как это условно показано светлым пунктиром на рис.2,а и на рис.2,г серыми линиями. Переход из состояния  $A$  в состояние  $\overline{A}$  происходит уже не скачком, а постепенно так же, как и переход из состояния  $\overline{A}$  в состояние  $A$ .

Постепенный переход означает, во-первых, что в промежуточной зоне оба состояния следует считать дробными (по крайней мере, в среднем). Для количественного обозначения долей состояний в каждой из переменных ( $A$ ,  $B$ ,  $C$ ,...) нам придется перейти от логических осей координат к непрерывным значениям вдоль математической оси на отрезке  $0 \div 1$ . На рис.2,д,е для иллюстрации показаны аналоговые переменные  $a_1$ ,  $b_1$  и  $c_1$  логических состояний, близких к '1', для переменных  $A$ ,  $B$  и  $C$ .

Во-вторых, следует признать, что сам переход может не быть полным (от целого состояния к целому) – он может начинаться в “целом”, а заканчиваться в промежуточном положении (рис.2,г). Тогда необходимы индексы '0' при

переменных ' $\overline{a}$ ,  $\overline{b}$ ,  $\overline{c}$ , ...' и '1' при переменных 'a, b, c, ...', которые показывают, откуда начался переход и где он заканчивается (показано стрелками на рис.2,г), а также насколько меньшими единицы стало их значение. Тот же индекс из двух ставится и у альтернативной переменной (на рис.2,г – нижняя пара –  $a_0$  и  $a_1$ ) “проникшей” в основную (классическую) переменную за счет нечеткости границ.

Логические величины дискретны (единичны) именно в силу своей различимости. Они отстоят друг от друга, как минимум, на порог восприятия [2÷4]. Поэтому наличие, кроме целого А, еще и дробных 'a' и  $\overline{a}$  совсем не означает, что последние могут быть обнаружены прямо. Если состояния А и  $\overline{A}$  отстоят друг от друга на порог восприятия, то тогда 'a' и  $\overline{a}$  - подпороговые и восприниматься могут только А или  $\overline{A}$ . Понятно, что при наличии шума, который может делать подпороговый сигнал надпороговым или надпороговый – подпороговым, появление А или  $\overline{A}$  должно носить случайный характер. Причем при “передвижении” вдоль переходной области к своему антиподу интенсивность появления исходного состояния будет падать (как показано на рис.2,г “исчезающим” пунктиром), а интенсивность появления его антипода – нарастать. Как видим, такие не совсем обычные – непредсказуемо проявляющие себя состояния 'a' и  $\overline{a}$ , вполне уместно назвать виртуальными (возможными) состояниями логических переменных А и  $\overline{A}$ .

Непрерывными в переходной области являются только линии вероятности изменения А -  $P_A$  и  $\overline{A}$  -  $P_{\overline{A}}$  (серые линии на рис.2,г). Очевидно, что в сумме они должны давать единицу:  $P_A + P_{\overline{A}} = 1$ . Сказанное выше дает основание утверждать, что линии вероятности должны быть не только непрерывными, но и плавными, т.е. они не должны содержать изломов - скачков в первой производной, что отражено на рис.2,г. Это значит, что линия вероятности перехода должна описываться кривой, как минимум, второго порядка.

Рассмотрим подробнее переход от '1' к '0' (рис.2,г). В ортогональных классических координатах А,  $\overline{A}$  – рис.2,ж, виртуальные  $a_1$  и  $\overline{a_1}$  не могут быть проекциями точки с прямой линии '1', соединяющей А и  $\overline{A}$  (показанной пунктиром), ибо тогда и линии вероятности  $P_A$  и  $P_{\overline{A}}$  на рис.2,г будут прямыми (и будут содержать излом). Значит, следует считать, что  $a_1$  и  $\overline{a_1}$  являются проекциями с окружности '2' (она показана непрерывной линией). Тогда для состояния А виртуальные состояния  $a_1$  и  $\overline{a_1}$  являются квадратными корнями или радикалами вероятности:  $a_1^2 = P_{AA}$  и  $\overline{a_1}^2 = P_{\overline{A}\overline{A}}$ , причем:

$$a_1^2 + \overline{a_1}^2 = 1. \quad (1,a)$$

Для перехода от '0' к '1' на рис.2,г картина полностью аналогична. Для состояния  $\overline{A}$  виртуальные состояния  $\overline{a_0}$  и  $a_0$  также есть *радикалы вероятности*:  $\overline{a_0^2} = P_{\overline{AA}}$  и  $a_0^2 = P_{AA}$ , причем:

$$\overline{a_0^2} + a_0^2 = 1. \quad (1,б)$$

Соотношения (1,а,б) имеют общий вид:

$$\overline{a^2} + a^2 = 1. \quad (1,в)$$

Попутно отметим, что *радикалом* является и огибающая сигнала: *радикалами мощности*  $P=I^2 \cdot R=U^2/R$ , “с точностью” до  $\sqrt{R}$ , служат ток  $I$  или напряжение  $U$  ( $R$  - сопротивление). Радикалы в отличие от своих квадратов имеют знакопеременные значения и складываются алгебраически – с учетом знака, т.е. соответствующие им физические величины обладают способностью к интерференции [4, 7].

На рис.2,з приведен полный набор 2-мерных состояний ( $n=2$  для  $A$  и  $B$ ). В отличие от своего классического прототипа на рис.2,б он имеет не  $2^n=4$ , а  $2^n \cdot 2^n=16$  состояний. Нетрудно видеть, что полная карта Вейча является двухуровневой: каждая крупная клетка, которая на рис.2,б изображала классическое состояние, теперь включает группу из 4-х виртуальных состояний. Одно виртуальное состояние в каждой группе является наследником или подпороговым остатком комбинации тех же логических переменных, что и в классике; например,  $b_1 a_1$  есть *наследник*  $BA$ . Три оставшиеся виртуальных состояния в этой клетке являются пересекающимися с  $BA$  соседних с ней клеток  $\overline{B A}$ ,  $\overline{B A}$ ,  $\overline{B A}$  в двухмерном пространстве. Состояния-наследники помечены на карте тем же цветом, что и их “родители”. Остальные виртуальные состояния оставлены бесцветными (вообще говоря, их цвет должен быть переходным, как и на рис.2,в, но передать это малоцветной машинной графикой затруднительно).

Как мы выяснили выше, для виртуальных состояний двух переменных справедливы следующие соотношения:

$$\overline{a_0^2} + a_0^2 = 1, \quad \overline{a_1^2} + a_1^2 = 1; \quad (2,а,б)$$

$$\overline{b_0^2} + b_0^2 = 1, \quad \overline{b_1^2} + b_1^2 = 1. \quad (3,а,б)$$

Чтобы образовать из них 4 комбинационные группы (рис.2,з), надо перемножить:  $(2,а) \cdot (3,а)$ ,  $(2,б) \cdot (3,а)$ ,  $(2,а) \cdot (3,б)$  и  $(2,б) \cdot (3,б)$ . Тогда получим следующую систему уравнений для групп  $\overline{B A}$ ,  $\overline{B A}$ ,  $\overline{B A}$ ,  $BA$ :

$$00: \overline{b_0^2} \cdot \overline{a_0^2} + \overline{b_0^2} \cdot a_0^2 + b_0^2 \cdot \overline{a_0^2} + b_0^2 \cdot a_0^2 = 1, \quad (4,а)$$

$$01: \overline{b_0^2} \cdot \overline{a_1^2} + \overline{b_0^2} \cdot a_1^2 + b_0^2 \cdot \overline{a_1^2} + b_0^2 \cdot a_1^2 = 1, \quad (4,б)$$

$$10: \overline{b_1^2} \cdot \overline{a_0^2} + \overline{b_1^2} \cdot a_0^2 + b_1^2 \cdot \overline{a_0^2} + b_1^2 \cdot a_0^2 = 1, \quad (4,в)$$

$$11: \overline{b_1^2} \cdot \overline{a_1^2} + \overline{b_1^2} \cdot a_1^2 + b_1^2 \cdot \overline{a_1^2} + b_1^2 \cdot a_1^2 = 1. \quad (4,г)$$

которая описывает значения вероятностей в каждой группе виртуальных состояний на рис.2,з (сумма остается по-прежнему равной единице). Соотношения (4,а÷г) имеют общий вид:

$$\overline{b^2} \cdot \overline{a^2} + \overline{b^2} \cdot a^2 + b^2 \cdot \overline{a^2} + b^2 \cdot a^2 = 1, \quad (4,д)$$

Для  $n > 2$  представление виртуальных состояний в виде “плоской” карты Вейча становится ненаглядным. Тогда имеет смысл перейти к обычной таблице, столбцы которой соответствуют коду задаваемого состояния VA-Set, а строки – коду VA-Get, обнаруживаемому при опросах – рис.2,и. Один столбец таблицы соответствует одной виртуальной группе на полной карте Вейча и одному из уравнений (4,а)÷г). Состояния-наследники образуют основную диагональ таблицы, идущей снизу вверх и направо; только эта диагональ присутствует в таблице для классических состояний.

В классической алгебре логики, задав, например, VA=10 можно быть уверенным, что и при опросе будет получен двоичный код 10. В реальности это далеко не всегда так: мы можем получать для каждого из 4-х значений входного Set-кода от 2-х до 4-х виртуальных значений выходного Get-кода с той или иной вероятностью (4), конечно, не одновременно, а в 2-х, 4-х или большем количестве последовательных считываний. В частном, конкретном случае в столбце не обязательно присутствие только виртуальных состояний; часть состояний-наследников могут иметь вероятность равную единице, тогда остальные состояния в столбце будут отсутствовать.

Вероятности численно равны квадратам произведений значений виртуальных переменных, находящихся в каждой клетке карты или таблицы. В отличие от (4), для упрощения записи на рис.2,ж)÷л) знаки квадратов в каждой из клеток опущены, но напомним о них служат квадратные корни, условно поставленные у логических переменных C, B, A на фрагментах ж)÷л).

В примере на рис.2,ж) выбраны следующие числа:  $\overline{a_0} = a_1 = \overline{b_0} = b_1 = \sqrt{3/4}$ , тогда (1):  $a_0 = \overline{a_1} = b_0 = \overline{b_1} = \sqrt{1/4} = 1/2$ . При этом получатся следующие значения вероятности для карты на рис.2,з) или таблицы на рис.2,и):

$$(b_0 a_0)^2 = (\overline{b_0} \overline{a_1})^2 = (\overline{b_1} a_0)^2 = (\overline{b_1} \overline{a_1})^2 = 1/16,$$

$$(b_1 a_0)^2 = (\overline{b_1} \overline{a_1})^2 = (\overline{b_0} a_0)^2 = (\overline{b_0} \overline{a_1})^2 = (b_0 a_1)^2 = (b_0 \overline{a_0})^2 = (\overline{b_1} a_1)^2 = (\overline{b_1} \overline{a_0})^2 = 3/16,$$

$$(b_1 a_1)^2 = (\overline{b_1} a_0)^2 = (\overline{b_0} a_1)^2 = (\overline{b_0} \overline{a_0})^2 = 9/16.$$

В таблице на рис.2,и) числители дробей располагаются следующим образом:

Таблица 1

<b>Get</b>				<b>/ 16</b>
11	1	3	3	9
10	3	1	9	3
01	3	9	1	3
00	9	3	3	1
	00	01	10	11 <b>Set</b>

Сумма числителей в каждом столбце таблицы равна 16. Общий для всех знаменатель, также равный 16, показан в правом верхнем углу как '/16'. В силу выбранных соотношений:  $\overline{a_0} = a_1$ ,  $\overline{b_0} = b_1$ , сумма числителей по каждой из строк

тоже равна 16. Это приводит к симметрии чисел таблицы относительно основной диагонали.

Во втором примере – рис.2,к, все переменные равновероятны:  $\overline{a_0} = a_0 = \overline{b_0} = b_0 = a_1 = \overline{a_1} = b_1 = \overline{b_1} = 1/\sqrt{2}$ , тогда получим, что все виртуальные комбинационные состояния также равновероятны:  $p_i = 4/16$ .

В первом примере видно, что все состояния-наследники заметно выделяются по относительной интенсивности (в 3 и более раз). Но все же бывшие классическими состояния заметно размыты (по соседям - 9/16 уже заметно меньше единицы), т.е. налицо увеличение энтропии (беспорядка). Неудивительно, что для описания поведения размытых состояний, как и шума вообще, требуется значительно большее количество информации.

Приведем также таблицу вероятностей для 3-мерных виртуальных состояний (n=3) – рис.2,л. Она содержит уже не  $2^n=8$ , а  $2^{2n}=8 \cdot 8=64$  состояния, потому, что по отношению к классической, имеется квадратичная зависимость в числе виртуальных состояний. Для тех же чисел, что и в первом примере ( $\overline{a_0} = a_1 = \overline{b_0} = b_1 = \overline{c_0} = c_1 = \sqrt{3/4}$ ), будем иметь следующие числители дробей в таблице рис.2,л:

Таблица 2

Get	( ↓ числители ↓, знаменатель дроби ⇒ ) / 64							
111	1	3	3	9	3	9	9	27
110	3	1	9	3	9	3	27	9
101	3	9	1	3	9	27	3	9
100	9	3	3	1	27	9	9	3
011	3	9	9	27	1	3	3	9
010	9	3	27	9	3	1	9	3
001	9	27	3	9	3	9	1	3
000	27	9	9	3	9	3	3	1
	000	001	010	011	100	101	110	111 Set

Общий для всех знаменатель, равный 64, показан в верхнем углу как '/64'. Сумма числителей по всем столбцам, естественно, равна 64, поскольку суммарная вероятность в каждой виртуальной группе есть 1. Таблица 2, так же, как и Табл.1, обратима относительно основной диагонали. Повторим, что в классике эта диагональ наследников была бы заполнена единицами, а не дробями (хотя и приближенными к 1), все остальные числа были бы нулями.

Особенность виртуальных комбинационных состояний состоит в том, что при изменении значения вероятности одной из переменных меняется вероятность каждого комбинационного состояния в силу того, что имеется определенная – поразрядная связь между комбинационными состояниями. Поэтому, для описания поведения всех  $2^{2n}$  виртуальных состояний достаточно задать всего 2n-пар вероятностей в аналогово-логическом пространстве (по двум парам на каждую классическую логическую переменную – рис.2,г).

Классический и виртуальный регистры. Если в классическом регистре, имеющем n-разрядов, установить исходный код в виде '0' или '1' в каждом разряде, то на выходе получим этот же код в виде только одного из  $2^n$

возможных чисел. Если же в виртуальном регистре установить  $\overline{a} \approx a \approx \overline{b} \approx b \approx \overline{c} \approx c \dots \approx 1/\sqrt{2}$ , то за достаточно длинную (а при большом 'n' – очень длинную) серию считываний можно получить все возможные числа в диапазоне  $0 \div 2^n$  с почти равной интенсивностью их появления.

Смена нулевых или единичных значений тех или иных разрядов виртуального регистра обнаруживается только от опроса к опросу и носит внешне неупорядоченный, случайный характер. Однако, в таком регистре точно сохраняются вероятности (значения 'a', 'b', 'c', и т.д.), он также помнит исходный Set-код, который размывает. Вероятности размыва можно определить опытным путем при наборе достаточно большой статистики.

Итак, введение виртуальных состояний  $\overline{a_0}, a_0$  и  $\overline{a_1}, a_1$  есть введение вероятностей, т.е. количественной оценки возможностей их появления в виде воспринимаемых A или  $\overline{A}$ . Можно условно считать, что виртуальные состояния “существуют” все вместе и одновременно, поскольку возможности всегда существуют одновременно. Тем не менее, во время каждого считывания состояния, в процессе самореализации находится лишь один частный сценарий непредсказуемого поведения “шумовой линии”, но тому, что (или кто) считывает, не дано узнать детали ее поведения. В этом и состоит суть информационного порога – зоны неразличимости, порождающей незнание.

Единственным косвенным способом распознать наличие виртуальных состояний является точное (т.е. многократное и достаточно длительное) измерение интенсивности “неправильного”, с точки зрения классики, появления комбинаций значений разрядов на Get-выходе регистра, отличающихся от заданной комбинации на его Set-входе. Факт косвенного распознавания имеет место при наблюдении броуновского движения тел: глаз, даже вооруженный оптическим микроскопом, не в состоянии различить ни отдельных молекул жидкости, ни даже их скоплений (движущих пылинку), однако, хаотичность движения пылинки позволяет предположить существование виртуальных (для наблюдателя) частиц вещества.

### **Виртуальные совместные состояния**

До сих пор мы рассматривали сигналы с шумом (по энергии), где ограничения по скорости не были существенными. Теперь нам предстоит рассмотреть интегрированные сигналы, показанные в правой части на рис.1. нас будут интересовать сигналы, близкие или равные порогу по действию. В работе [4] показано, что для таких сигналов, вне их опорных точек, обязательен информационный шум, где характеристическим параметром является не энергия, а действие (т.е. он явно не классический).

Сигналы, показанные на рис.1, д÷е, практически полностью интегрированы. Если суммарный – составной сигнал близок к порогу, то нет возможности выделить его составляющие и сигналы следует рассматривать только совместно, как единое целое. Тогда и их состояния должны быть записаны в совместном виде, т.е. уравнение (4,д) следует записать так:

$$\langle \overline{b} \overline{a} \rangle^2 + \langle \overline{b} a \rangle^2 + \langle b \overline{a} \rangle^2 + \langle ba \rangle^2 = 1. \quad (5)$$

Здесь в каждой скобке находится не произведение частных вероятностей, как в (4,д), а некое единое обобщенное число, являющееся слагаемым вероятности совместного состояния. В силу подпороговости тут невозможно сказать, чему равна вероятность  $p_a$ ,  $p_b$  и т.д., определяемой является только обобщенная величина  $p_i$  ( $i \leq 2^n$ ). Для удобства, в записи (5) можно разделить функции идентификации состояния и задания численного значения его вероятности. Тогда (5) примет следующий вид:

$$r_1^2 \langle \overline{b} \overline{a} \rangle + r_2^2 \langle \overline{b} a \rangle + r_3^2 \langle b \overline{a} \rangle + r_4^2 \langle ba \rangle = 1, \quad (6,a)$$

или

$$(r_1^2 \langle \overline{a} \rangle + r_2^2 \langle a \rangle) \langle \overline{b} \rangle + (r_3^2 \langle \overline{a} \rangle + r_4^2 \langle a \rangle) \langle b \rangle = 1, \quad (6,b)$$

или, условно вынося за скобку 'b', а не 'a'

$$(r_1^2 \langle \overline{b} \rangle + r_3^2 \langle b \rangle) \langle \overline{a} \rangle + (r_2^2 \langle \overline{b} \rangle + r_4^2 \langle b \rangle) \langle a \rangle = 1; \quad (6,b)$$

здесь содержимое ' $\langle \rangle$ '-скобок есть идентификатор совместного состояния 'b' или  $\overline{b}$  с 'a' или  $\overline{a}$ , а их вероятности  $p_i$  задаются квадратами радикалов:  $r_i^2 = p_i$ .

При трех переменных левая часть уравнения растет экспоненциально и имеет  $2^3$  радикалов вероятности:

$$\begin{aligned} & \{(r_1^2 \langle \overline{a} \rangle + r_2^2 \langle a \rangle) \langle \overline{b} \rangle + (r_3^2 \langle \overline{a} \rangle + r_4^2 \langle a \rangle) \langle b \rangle\} \langle \overline{c} \rangle + \\ & + \{(r_5^2 \langle \overline{a} \rangle + r_6^2 \langle a \rangle) \langle \overline{b} \rangle + (r_7^2 \langle \overline{a} \rangle + r_8^2 \langle a \rangle) \langle b \rangle\} \langle c \rangle = 1. \end{aligned} \quad (7)$$

В соотношении (7), как и в (6,б,в), переменные можно менять местами произвольно ('c' не имеет приоритета над 'a' и 'b', соответственно, 'b' не имеет приоритета над 'a').

Сравнение комбинационных и совместных состояний. И те и другие виртуальные состояния имеют общие свойства, вытекающие из того, что они подпороговые:

- 1) виртуальные состояния не могут быть обнаружены прямо, их появление выглядит как шум – случайное появление классических состояний (шум дискретизации при аналого-цифровом преобразовании является отдаленной аналогией, по крайней мере, комбинационных состояний);
- 2) вероятностью появления виртуальных состояний можно управлять классическими средствами;
- 3) виртуальные состояния, в силу подпороговости, не могут сами управлять другими виртуальными состояниями (управление по шагам всегда остается классическим).

С другой стороны, имеются и различия: для того чтобы задать  $2^n$  совместных состояний необходимо  $2^n$  чисел, а для того чтобы задать те же  $2^n$  комбинационных состояний достаточно 'n' чисел, из которых составляется  $2^n$  комбинаций (произведений). В силу этого, уравнение (4,д) есть сумма произведений частных вероятностей каждой из переменных, оно является тождеством, т.е. выполняется для любых  $0 \leq a, b \leq 1$ . Это легко видеть, если записать (4,д) по аналогии с (6,б):

$$(\overline{a^2} + a^2)\overline{b^2} + (\overline{a^2} + a^2)b^2 = (\overline{a^2} + a^2)(\overline{b^2} + b^2) = 1. \quad (8)$$

Здесь  $\overline{a^2} + a^2 = 1$  (2) и  $\overline{b^2} + b^2 = 1$  (3), а из (6,а) следует, что  $(r_1^2 + r_2^2) < 1$  и  $(r_3^2 + r_4^2) < 1$ .

Уравнение (4,д) задает совокупность всех одновременно возможных комбинационных состояний; реализоваться могут не все из них (в классике реализуется только одно состояние из четырех). Однако, если комбинационное состояние  $[\overline{b} \cdot \overline{a} + b \cdot a]$  вполне осуществимо, то состояние  $[\overline{b} \cdot a + b \cdot \overline{a}]$  совсем невозможно: поскольку тогда  $\overline{b} \cdot a = 0$ , либо  $b \cdot \overline{a} = 0$ , а это приводит к отсутствию либо  $\overline{b} \cdot \overline{a}$ , либо  $b \cdot a$ . Совместное же состояние  $[\langle \overline{b} \cdot \overline{a} \rangle + \langle b \cdot a \rangle]$  вполне допустимо.

В использованной в квадратных скобках форме записи состояния арифметический знак '+' является скорее логическим знаком дизъюнкции; знак умножения '.' поставлен намеренно (хотя его можно опускать). Это сделано потому, что в форме  $\langle ba \rangle$ , запись 'ba' не является арифметическим произведением.

### Функции классических состояний

Попробуем перейти теперь к преобразованию одних состояний в другие для чего воспользуемся понятием функции  $y=f(x)$ . Если математическая функция непрерывна, то она имеет бесконечное число состояний аргумента и состояний функции. В функции, удовлетворяющей пороговому условию, количество состояний аргумента  $A_n$  и возможных состояний функции  $F_n$  конечно по определению, т.е. функция дискретна.

В обсуждаемом случае функция дискретна и имеет не один, а несколько независимых аргументов (A,B,...), поэтому удобней перейти к одной иерархической переменной [1] по оси абсцисс.

**Функции иерархических переменных.** Для подобного перехода надо разбить каждый интервал между соседними значениями одного из аргументов на меньшие интервалы - по числу значений второго аргумента (т.е. воспользоваться пустыми точками [1] первой переменной). Тогда, вместо двух, например, четырехзначных осей: 00, 01, 10, 11, мы получим одну числовую ось с шестнадцатью значениями: 00.00, 00.01, 00.10, 00.11; 01.00, 01.01, 01.10, 01.11; 10.00, 10.01, 10.10, 10.11; 11.00, 11.01, 11.10, 11.11 (точки и точки с запятой поставлены для большей наглядности разграничения переменных).

Интервал между соседними значениями второго аргумента можно также разбить на меньшие части - для третьего аргумента и так далее. Чем больше размерность (количество) и размер (длина кода) входных переменных, тем экспоненциально больше число требуемых шагов по иерархической оси аргументов.

Практически, мы уже пользовались двумя и тремя одноразрядными иерархическими Set-переменными в таблицах на рис.2,и,л; где сами таблицы для классических переменных выглядят (цветные клетки) как линейная функция тождественности  $y \equiv x$ , означающая повторение входных Set-состояний на Get-выходе.

Функции вычислений. Нас будут интересовать функции с иерархическим аргументом, отображающие (как, например, таблица умножения) результат арифметических или логических действий. На рис.3,а,б представлены две функции вычислений – сложения и умножения. Здесь на оси абсцисс присутствуют две арифметические переменные (дающие в сумме 16 значений). Как видим, расположение “опорных точек” [1,4] классической функции, отображаемое единицами, может быть произвольным, но оно должно содержать только  $2^n$  занятых клеток (остальные клетки нулевые, точнее пустые).

Таким образом, путем введения иерархической переменной производится преобразование многомерное пространства (аргументов) в одномерное, но со сложной – иерархической структурой. Некоторой особенностью такой структуры является то, что в ней все аргументы равноправны – находясь, формально, на разных уровнях иерархии они вполне могут меняться местами.

### **Функции виртуальных комбинационных состояний**

Как мы выяснили выше, наличие виртуальных состояний существенно – квадратично расширяет объем занимаемого состояниями логического пространства. Действительно, как показано на рис.2,и,л, задавая (Set)  $2^n$  комбинаций, мы получаем при опросе (Get)  $2^{2^n}$  комбинаций – по  $2^n$  на каждую установленную.

Поэтому вполне понятно желание [8] использовать дополнительное пространство виртуальных состояний для построения в нем функций, которые могут иметь гораздо большее число состояний в каждом отсчете по оси абсцисс. Дело, однако, в том, что если классические состояния можно задавать, т.е. устанавливать, и затем получать заданную комбинацию при считывании, то виртуальные состояния не управляемы. Каждое из них невозможно ни установить в обычном понимании, ни прямо обнаружить при считывании. Тем не менее, и здесь имеется один управляемый параметр, который можно задавать – это вероятность появления виртуальных состояний.

Это значит, что по оси ординат можно использовать значения вероятности 'р' получения состояний при опросе (рис.3,в,г). К сожалению, участок, на котором “работает” вероятность комбинационных состояний, локализован; он не охватывает всех  $2^{2^n}$  комбинаций, а только  $2^n$  из них (образующих одну группу на диаграмме рис.2,з или один столбец в таблицах на рис.2,и,л). Для каждой из этих групп сумма всех отсчетов значений вероятности равна единице.

В пределах одной (или каждой) группы нетрудно вообразить вероятностную функцию вычисления суммы (рис.3,в) или произведения (рис.3,г), аналогичные классическим функциям на рис.3,а и рис.3,б. Очевидно, что масштаб представления выходных значений функции должен быть нормирован так, чтобы их сумма давала единицу.

**Ограничения вероятностных комбинационных функций.** О первом ограничении мы только что сказали: наличие 'а<sub>0</sub> и а<sub>1</sub>,...' (наличие  $2^n$  столбцов в таблицах на рис.2,и,л) не дает дополнительных возможностей построения требуемых функций через вероятности.



Второе ограничение вытекает из того факта, что используя 'n' переменных нельзя предопределить  $2^n$  значений произвольной функции, точнее, определить можно, но эти значения не будут независимыми от других. Покажем это на примере. Любое из уравнений (4) может быть записано через вероятности виртуальных состояний следующим образом:

$$p_1 + p_2 + p_3 + p_4 = 1. \quad (9)$$

где, с учетом (2) и (3):

$$p_1 = (1-b^2) \cdot (1-a^2), \quad p_2 = (1-b^2) \cdot a^2, \quad (10,а,б)$$

$$p_3 = b^2 \cdot (1-a^2), \quad p_4 = b^2 \cdot a^2. \quad (10,в,г)$$

Получается, что если мы вычислим 'a' и 'b' из (10,а,б), то  $p_3$  и  $p_4$  будут иметь принудительно заданные значения.

Ограничения указанного вида не позволяют реализовать произвольную вероятностную функцию вычисления.

### Функции виртуальных совместных состояний

Радикалы вероятности  $r_i$  (6,7) при совместных состояниях  $\langle \bar{c} \bar{b} \bar{a} \rangle \dots \langle cba \rangle$  являются относительно свободными и независимыми числами (эта свобода ограничена лишь общим условием, что сумма их квадратов должна быть равна единице). Поэтому с помощью набора  $r_i$  может быть реализована любая *функция вероятности*. Повторим, что платой за свободу поведения функции вероятности *совместных состояний* является то, что необходимо задавать все  $2^n$  чисел, а не  $n$ -чисел, как для *комбинационных состояний*, где этой свободы нет.

На рис.4,а показан пример функции NOT, действующей на младший разряд регистра, находящегося в исходном Set-состоянии '00' и переходящий в Get-состояние '01'. На рис.4,б младший разряд переводится в равновероятное виртуальное состояние из состояния '1' ( $H_1$ ), а на рис.4,в и старший разряд (с учетом нового состояния младшего) переводится в равновероятное виртуальное состояние из состояния '0' ( $H_2$ ), цифры в клетках есть радикалы вероятностей. Наконец, на рис.4,г к полученному на 3-м шаге состоянию еще раз применяется преобразование  $H_1$ . Функция на этом шаге имеет по 2 значения в одном ряду, поэтому здесь происходит интерференция виртуальных состояний, поскольку состояния аргумента также виртуальны.

**Влияние интерференции на Get-состояния.** На рис.4,д приведен пример “виртуальной” функции, прототипом которой служит классическая линейная функция тождественности  $F_n \equiv A_n$  (показана цветом). Как видим, при наличии виртуальных состояний функция является многозначной; многозначным может быть и исходное состояние (аргумент функции).

Если  $A_n$ -состояния '00' или '01' задаются классическим образом, то для функции  $F_n$  на рис.4,д, считываться в первом случае будет:  $\sqrt{1/2} [\langle 00 \rangle + \langle 01 \rangle]$ , а во втором:  $\sqrt{1/2} [\langle 00 \rangle - \langle 01 \rangle]$ . Если же задаются  $A_n$ -состояния '10' или '11', то считываться будет:  $\sqrt{1/2} [\langle 10 \rangle + \langle 11 \rangle]$  и  $\sqrt{1/2} [\langle 10 \rangle - \langle 11 \rangle]$ .

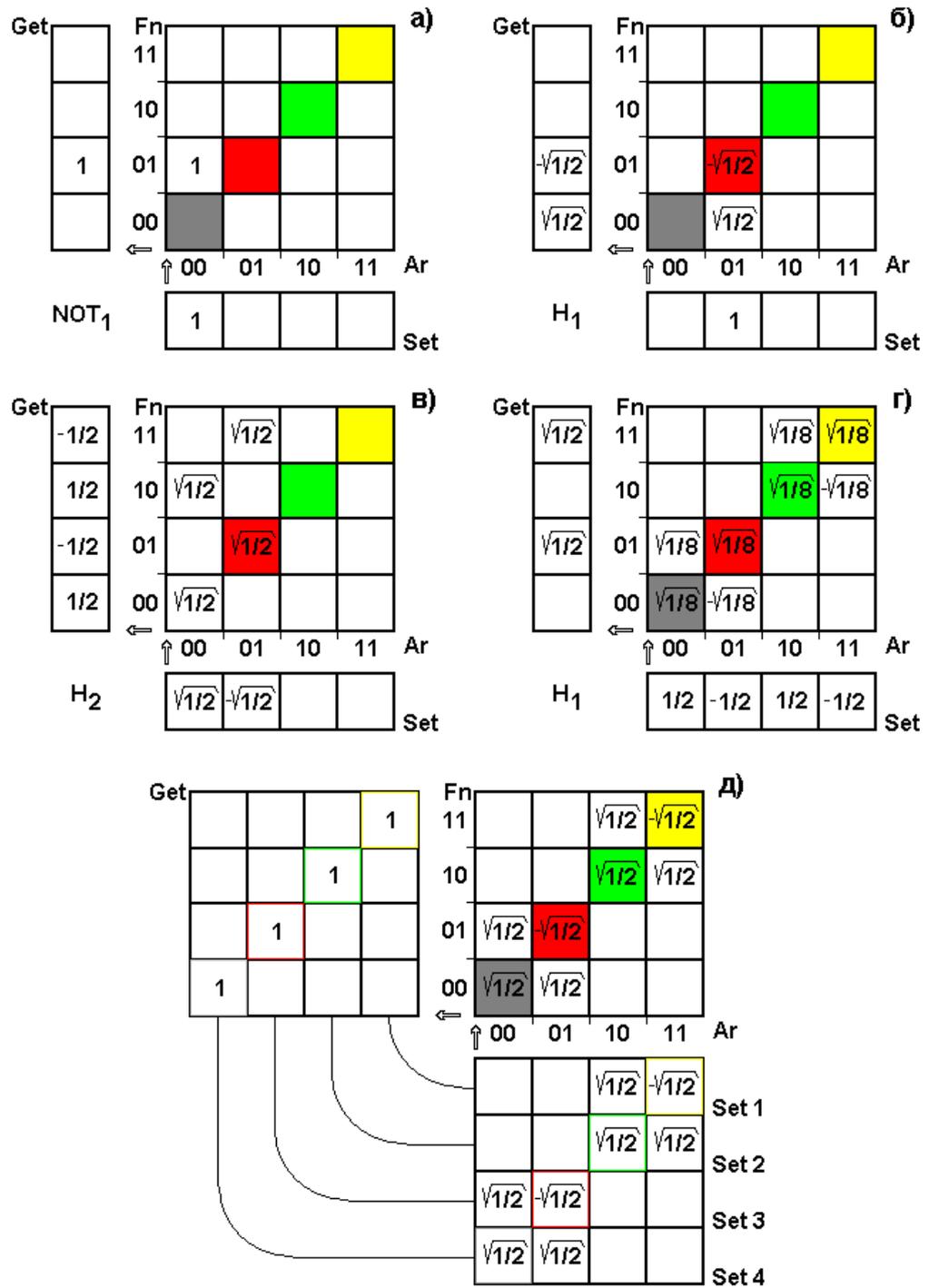


Рис.4,а÷г) четыре последовательных изменения состояния с помощью функции преобразования Fn, исходным является состояние '00' (цифры в клетках есть радикалы вероятностей); Set-радикалы перемножаются по столбцам, Get-радикалы складываются по рядам;

д) четыре независимых изменения различных виртуальных состояний, показанных для удобства вместе. Прототипом функции Fn является функция тождественности (отмечена цветом), Get-состояния принимают те же значения, что и классическая функция-прототип.

В г) и д) наглядно видно действие интерференции виртуальных состояний.

Посмотрим, что получится, если исходное Set-состояние тоже виртуально и равно  $\sqrt{1/2} [\langle 00 \rangle + \langle 01 \rangle]$ . Тогда будем иметь при считывании следующее Get-состояние:

$$\sqrt{1/2} [\sqrt{1/2} \langle 00 \rangle + \sqrt{1/2} \langle 01 \rangle] + \sqrt{1/2} [\sqrt{1/2} \langle 00 \rangle - \sqrt{1/2} \langle 01 \rangle] = \langle 00 \rangle. \quad (11,а)$$

Если же исходное Set-состояние равно  $\sqrt{1/2} [\langle 00 \rangle - \langle 01 \rangle]$ , то получим:

$$\sqrt{1/2} [\sqrt{1/2} \langle 00 \rangle + \sqrt{1/2} \langle 01 \rangle] - \sqrt{1/2} [\sqrt{1/2} \langle 00 \rangle - \sqrt{1/2} \langle 01 \rangle] = \langle 01 \rangle. \quad (11,б)$$

Если исходное Set-состояние равно  $\sqrt{1/2} [\langle 10 \rangle + \langle 11 \rangle]$ , тогда Get-состояние:

$$\sqrt{1/2} [\sqrt{1/2} \langle 10 \rangle + \sqrt{1/2} \langle 11 \rangle] + \sqrt{1/2} [\sqrt{1/2} \langle 10 \rangle - \sqrt{1/2} \langle 11 \rangle] = \langle 10 \rangle. \quad (11,в)$$

Наконец, если исходное Set-состояние равно  $\sqrt{1/2} [\langle 10 \rangle - \langle 11 \rangle]$ , то получим:

$$\sqrt{1/2} [\sqrt{1/2} \langle 10 \rangle + \sqrt{1/2} \langle 11 \rangle] - \sqrt{1/2} [\sqrt{1/2} \langle 10 \rangle - \sqrt{1/2} \langle 11 \rangle] = \langle 11 \rangle. \quad (11,г)$$

Как видим

- а) интерференция радикалов вероятности меняет состояние выхода (в этом смысле знак радикала вероятности есть свободный параметр для влияния на результат, в дополнение к численному значению самого радикала);
- б) в результате, (в выбранном примере) Get-состояния совпадают с теми, которые были бы у классической функции при классических Set-состояниях (отмечены цветными рамками на рис.4,д).

Заметим, что если Set-состояния заданы точно, то и Get-состояния '0' и '1' будут заданы точно, а не в среднем, как все промежуточные виртуальные состояния. В этом случае можно говорить о восстановлении классических состояний, которые были размыты виртуальным шумом.

**Непредсказуемость реализации вероятности.** Показанная на рис.3,в и рис.3,г, вероятностные функция сложения и умножения, как и любые другие функции целочисленного аргумента, могут существовать и при наличии совместных виртуальных состояний. Появилась, однако, одна “небольшая” неприятность – значение вероятности не может быть получено за одно обращение в принципе – для этого необходимо предпринять множество попыток (так же впрочем, как и при комбинационных состояниях). Таких попыток (измерений) придется сделать тем больше, чем больше необходимая точность установления вероятности (не путать установление с установкой). Очевидно, что это ограничение существенно понижает скорость достижения результата, равно как и привлекательность обсуждаемого способа вычислений. Поэтому о быстрых вычислениях по произвольным алгоритмам через функции вероятности можно забыть.

К подобному же выводу можно прийти, рассматривая задачу с чисто классических позиций. Случайное появление неправильных результатов при измерении выглядит в классике как некоторый шум, порождающий ошибки. Этот шум, в отличие от классического, нельзя свести к пренебрежимо малому уровню путем усреднения. Повторными измерениями можно лишь достаточно точно выяснить вероятности отклонений от классики. В экспериментальной физике это процедура широко известна и называется “набором статистики”.

Скорость набора статистически обеспеченной информации при наличии шумов, естественно, получается весьма низкой.

Тем не менее, имеется один класс задач, где ситуация в корне меняется – это задачи на поиск максимума какой-либо функции. У вероятностной функции максимум соответствует наиболее вероятному состоянию и его не надо ждать долго – такое состояние само появляется одним из первых.

Таким же образом могут быть найдены и максимумы периодически повторяющихся функций с достаточно острыми пиками. Если максимумы гладкие (как, например, в синусоиде) или пиков слишком много, то можно перейти к спектру исследуемой функции (используя преобразование Фурье) и получить один общий пик вероятности, соответствующий обратному значению периода (точнее, речь идет о первом, отстоящем от нуля пике Фурье-спектра – рис.5,б). Следовательно, задачи, где можно использовать нахождение (среднего) периода повторений каких либо процессов также могут решаться достаточно эффективно с помощью обсуждаемого метода.

### Совместные состояния в микромире

Из изложенного выше очевидно, что существование виртуальных состояний прямо следует из ограничений быстроты и энергии восприятия сигналов. Проявление ограниченности быстроты изменений весьма характерно для микромира [4]. Рассмотренная во введении прозрачность узкого потенциального барьера (туннельный эффект) служит наглядной иллюстрацией этому.

В настоящее время в квантовой механике активно обсуждаются способы реализации вычислений с использованием суперпозиционных состояний кубитов [9,10], позволяющие экспоненциально повысить скорость решения некоторых задач. Точнее говоря, целью является достижение хотя бы степенного роста времени решения экспоненциальных задач (задач, в которых при увеличении “размера” входных переменных экспоненциально растет число выполняемых действий).

Наличие суперпозиционных состояний также следует из быстрой пороговых информационных ограничений. Выведенные нами из факта существования порога по действию совместные виртуальные состояния и есть не что иное как суперпозиционные состояния, а функция преобразования состояний  $F_n$  (рис.3 и рис.4) это матрица преобразования  $U(2^n \times 2^n)$ . Примечание: логическая функция преобразования есть гейт, а разряд виртуального регистра – кубит.

В силу отмеченных выше негативных особенностей вероятностных функций, вычислительных задач в “квантовой реализации” предложено не так уж много. Наиболее выигрышно решается задача факторизации (разложения на 2 простых множителя) целого числа  $M$ , потому, что она сводится алгоритмом Ленстры [11] к поиску периода вспомогательной функции  $f(m) = u^m \bmod M$ , определяемой в области, лежащей от  $M^2$  до  $2M^2$  ('mod  $M$ ' означает остаток от деления  $u^m$  на  $M$ ). Пример такой функции для  $M=15$ ,  $u=2$  показан на рис.5,а (' $u$ ' выбирается произвольно).

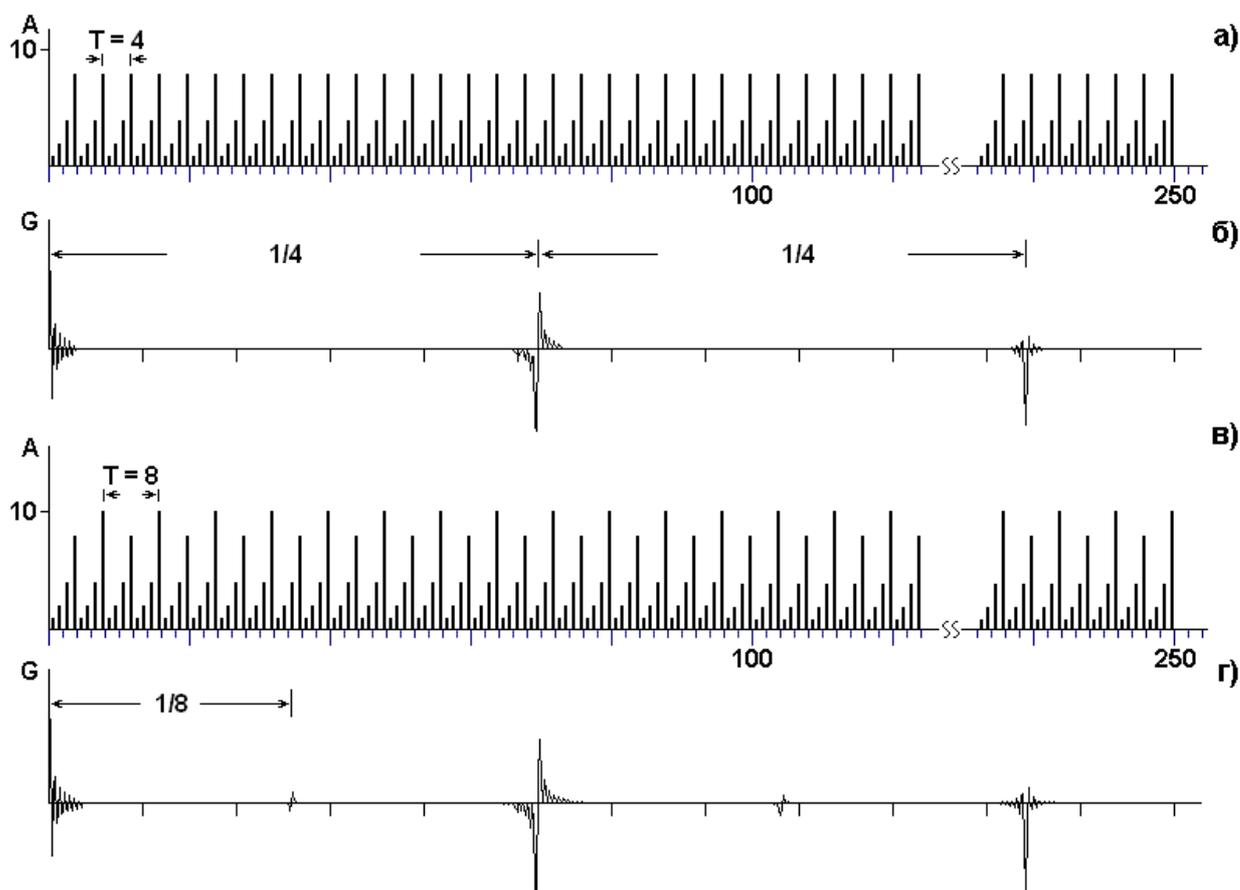


Рис.5,а) – периодическая целочисленная функция “1-2-4-8” для  $M=15$ ,  $u=2$  имеет в Фурье-спектре – б) пик на нулевой гармонике – в силу наличия постоянной составляющей. Спектр образован суммой 250 косинусов ( $M^2=225$ ); его пики отстоят друг от друга на интервалы, обратные величине периода.

На фрагменте в) показана периодическая функция “1-2-4-8-1-2-4-10”; максимумы пиков ее Фурье-спектра по-прежнему идут с шагом  $1/T$ , а пики соответствующие периоду ( $1/8$ ) весьма малы. Это значит, что в алгоритме Шора [10] эти пики не будут наиболее вероятными.

Почти все действия, входящие в алгоритм Ленстры, осуществляются классическими методами. Следует отметить, что 'm' по порядку величины соответствует  $M^2$  (это область определения вспомогательной функции). Значения M, при которых реализация алгоритма Ленстры классическими средствами становится нереально долгой, оцениваются на уровне  $2^{1000}$  [13,14]. При таком диапазоне даже вычисление самих значений вспомогательной функции ( $2^{1000}$  слов разрядностью до  $\sim\sqrt{M}$ ) может стать достаточно трудоемкой процедурой.

Методами квантовой механики находится только период повторения функции  $f(m)$  через преобразование Фурье – рис.5,б с использованием, так называемого квантового параллелизма [10], который есть не что иное, как наличие у частиц микромира набора *совместных* виртуальных состояний. Считается, что задача нахождения периода всегда ведет к экспоненциальному росту числа действий при росте диапазона значений аргумента вспомогательной функции – m ('m' стоит в  $f(m)$  в показателе степени). Вообще говоря, слово “всегда” здесь не всегда уместно. Из приведенных на рис.5,а,в примеров видно, что период вполне может быть найден как расстояние между пиковыми значениями функции, а эта задача не экспоненциальная и ее можно попутно решить при вычислении значений вспомогательной функции  $f(m)$ . Хотя, конечно, нетрудно себе представить медленную периодическую функцию в смеси с частыми периодическими пиками большой амплитуды, где период по пикам будет определяться неверно. При практическом решении задачи факторизации, вполне можно начать с классического пути решения и в качестве первого шага попытаться определить период по пикам, тем более что проверка правильности решения в обсуждаемой задаче достаточно проста.

**Управление вероятностью совместных состояний.** Управлять вероятностью комбинационных виртуальных состояний сравнительно просто – путем изменения значений частных вероятностей 'a,b,c,...' и сравнительно легко, поскольку частных вероятностей немного ('n', а не  $2^n$ ).

В совместных виртуальных состояниях придется прямо задавать все  $2^n$  вероятностей, но тогда задачи, связанные с нахождением пика вероятности практически лишаются смысла – ведь уже приготавливая эти  $2^n$  значений, легко узнать какое из них максимально. Поэтому из двух типов указанных выше возможных для вычислений через вероятности задач, остаются только задачи второго типа, связанные с нахождением периода функций.

Однако, цитируя [14], “Управление работой квантового компьютера с 'n' кубитами описывает преобразование  $|\psi_f\rangle = U(2^n \times 2^n)|\psi_{in}\rangle$ . При значениях  $n \approx 10^3$  умножение  $U|\psi_{in}\rangle$  становится недоступным для самых быстрых (порядка  $10^{12}$  операций в секунду) компьютеров. Еще более трудной представляется физическая реализация преобразования  $|\psi_f\rangle \rightarrow |\psi_{in}\rangle$ ”. Примечание:  $|\psi_{in}\rangle$  и  $|\psi_f\rangle$  есть аналоги Set-входа и Get-выхода.

Предлагаемое решение [15] состоит в разложении матрицы  $U(2^n \times 2^n)$  на произведение матриц второго и четвертого порядков:

$$U(2^n \times 2^n) = \prod_{i,j} U_i(2 \times 2) \otimes U_j(2^2 \times 2^2), \quad (12)$$

здесь числа множителей  $i, j$  определяют число однокубитовых и двухкубитовых операций, необходимых для реализации алгоритма. Однако, не каждый из алгоритмов преобразования состояний является эффективным потому, что число операций все равно может возрастать экспоненциально с “размером задачи”. Там же, где достигается снижение числа операций, переход к произведению матриц близок, по сути, к управлению в комбинационном стиле.

### Способы реализации виртуальных состояний

Из обычного классического регистра вполне можно создать регистр – рис.6,а, обладающий виртуальными состояниями, т.е. дающий шумовое размытие считываемых состояний. Для этого надо в каждом разряде подключить мультиплексор  $M$  к выходам триггера  $T1$  (рис.6,а) и попеременно, с заданной вероятностью, подключать на выход мультиплексора состояние  $Q$  либо  $\overline{Q}$  триггера.

Общий для всех разрядов регистра тактирующий генератор служит для инкрементации счетчика  $\Sigma$ . Значение  $\Sigma_{\text{макс}}$  есть максимально возможное число шагов управления скважностью (напомним, что скважность есть отношение длительности импульса к периоду). Период циклов повторения работы схемы задается сигналом переполнения счетчика, формируемым по длительности. Сигнал переполнения устанавливает (в единицу – по входу  $S$ ) вспомогательный триггер  $T2$ , который управляет переключением мультиплексора.

Когда число на выходе счетчика станет равным заданному коду скважности (в пределах  $1 \div \Sigma_{\text{макс}}$ ) схема сравнения кодов сбросит триггер  $T2$ . Таким образом, на выходе  $T2$  можно получать импульс изменяемой длительности от  $1/\Sigma_{\text{макс}}$  до  $(\Sigma_{\text{макс}}-1)/\Sigma_{\text{макс}}$  периода циклов. В этих же границах будет регулироваться доля периодического присутствия  $Q$  либо отсутствия  $\overline{Q}$  на виртуальном выходе.

Настраивая в каждом разряде величину скважности можно менять вероятность считываемых альтернативных состояний. Чтобы выходной Get-код носил случайный характер, опрос регистра следует производить с достаточно размытым периодом, намного большим, чем период общего генератора циклов.

При частоте тактового генератора  $f_T=100\text{МГц}$ , числе шагов регулирования вероятности  $\Sigma_{\text{макс}}=1024$  (10 разрядов в счетчике), период повторения циклов общего генератора, т.е. гарантированный период появления нового виртуального состояния, составит  $\sim 10$  мкс. Делая опросы случайным образом, в среднем раз за 1000 периодов, за 10 секунд имеется возможность зафиксировать до 1 тысячи состояний в поиске наиболее вероятного. Сам по себе опрос должен выполняться за один период тактового генератора (т.е. за 10 нс) синхронно по всем разрядам.

На рис.6,б,в показаны временные диаграммы работы двух разрядов такого регистра, вероятности виртуальных состояний которых соответствуют рис.2,к и рис.2,ж, соответственно. Во втором случае последовательность вероятностей: 1, 3, 9, 3, соответствует вероятностям состояний первой строки Табл.1.

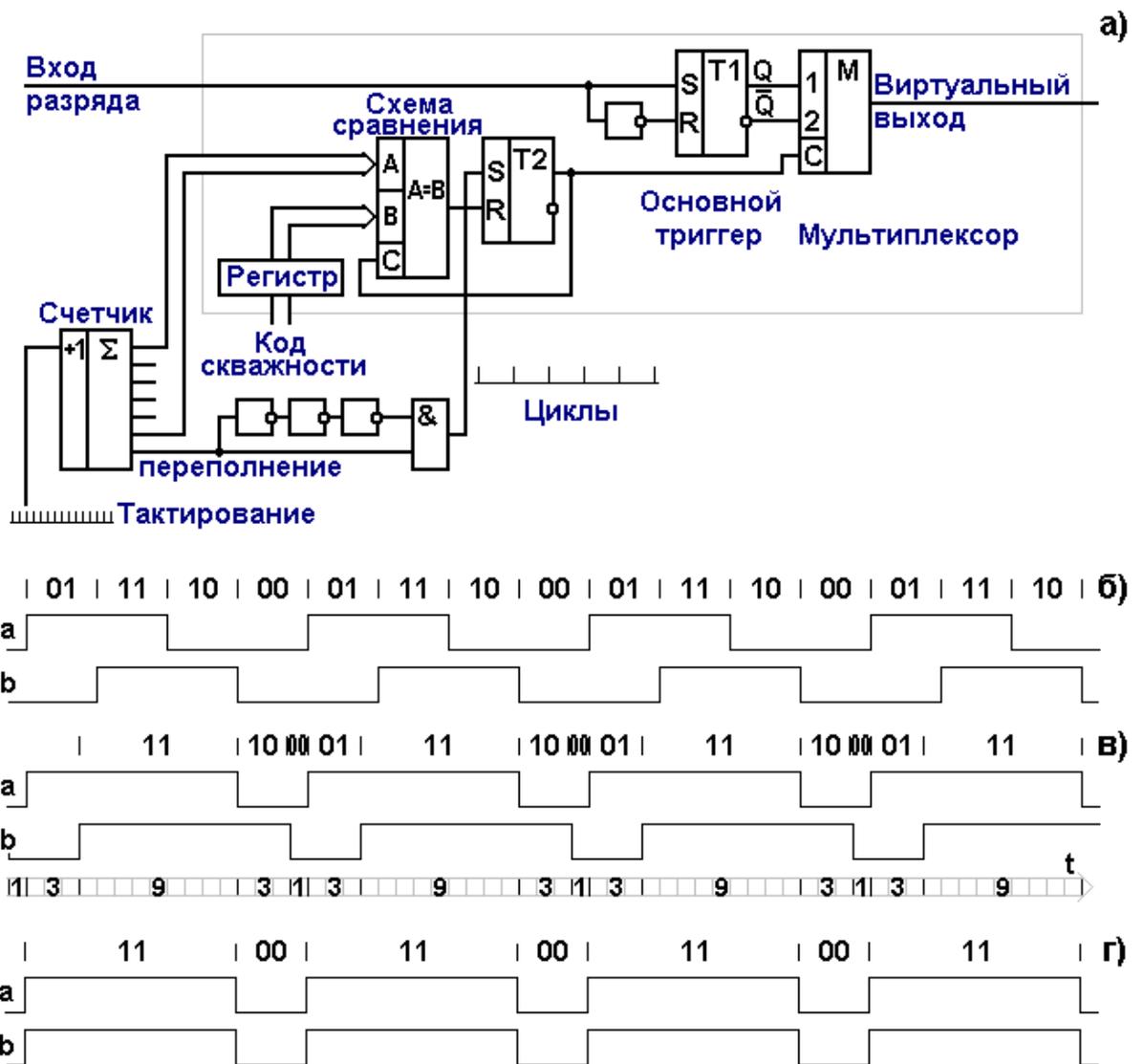


Рис.6,а) функциональная схема одного разряда виртуального регистра (обведен серой рамкой) с цифровым заданием скважности чередования состояний '0' и '1' на выходе в каждом цикле. Максимальное число на выходе счетчика -  $\Sigma_{\text{макс}}$  должно быть равно требуемому количеству дискретных шагов изменения вероятности (в пределах от '0' до '1'). Соответственно, скважность регулируется в численных границах: от  $1/\Sigma_{\text{макс}}$  до  $(\Sigma_{\text{макс}}-1)/\Sigma_{\text{макс}}$ . Узлом управления вероятностью является регистр, куда записывается код скважности. Опрос виртуального выхода должен производиться в течение одного такта в случайные моменты времени относительно циклов работы схемы.

б) работа двух регистров с равновероятными виртуальными состояниями у каждого;

в) работа двух регистров с вероятностями виртуальных состояний 3/4 и 1/4 у каждого (Табл.1);

г) управляя фазой между циклами 'a' и 'b' можно получить “запутанные” совместные состояния  $\{ \langle 00 \rangle + \langle 11 \rangle \}$ .

Представленная схема является лишь окончательным устройством, реализующим “параллелизм возможностей” виртуальных комбинационных состояний. Вероятности в ней задаются непосредственно, а не с помощью радикалов, все манипуляции с которыми (включая интерференцию) можно проводить предварительно программными методами.

Заметим, что управляя фазой между циклами 'a' и 'b' можно получить показанные на рис.6,в “запутанные” совместные состояния  $[\langle 00 \rangle + \langle 11 \rangle]$ , невозможные в комбинационных сочетаниях.

Оценка затрат на реализацию. Для построения простого RS-триггера T1, включая логику управления, достаточно всего 4-х логических вентилях (2÷3-входных логических схем) и в ~2 раза больше вентилях необходимо для мультиплексора M. Поэтому аппаратные ресурсы будут потрачены не столько на основной триггер и мультиплексор, сколько на построение схемы управления скважностью.

Для хранения кода скважности в каждом разряде потребуется  $4\Sigma_{\text{макс}}$  вентилях. Схема сравнения также займет ~4 вентилях на каждый из  $\Sigma_{\text{макс}}$  разрядов. Всего потребуется  $8\Sigma_{\text{макс}}$  вентилях (затраты на триггер T2 пренебрежимо малы). При  $\Sigma_{\text{макс}} \approx 1000$  это составит 8000 вентилях на схему управления скважностью, а всего на 1 разряд регистра, добавляя 500 вентилях на узел ввода-вывода кода скважности, получим ~8500 вентилях.

В целом, для регистра разрядностью  $B=1000$  потребуется 8500000 логических вентилях. Считая, что в одном вентиле находится ~10 транзисторов, а в одном корпусе большой интегральной схемы (БИС) размещается несколько миллионов транзисторов, получим, что вычислитель разместится в 20÷30 БИС. Как видим, даже при лобовом решении задачи, количество необходимых БИС вполне приемлемое.

## **Заключение**

В теории сигналов до сих пор мало изучалось восприятие по действию в силу убеждения, что информацию следует передавать “по энергии” – только в пределах основной полосы частот для того, чтобы обеспечить существенное превосходство сигнала над шумом (хотя классический шум за пределами основной полосы интегрируется, т.е. сходит к нулю, поскольку постоянной составляющей у него нет). Только в наносекундной ядерной электронике существует не совсем адекватное понятие “зарядовой” чувствительности регистратора, размывающей его время срабатывания при разбросе амплитуд (ступенчатых) сигналов. Видимо поэтому, понятие порога по действию не было выработано до последнего времени, хотя это вполне можно было сделать десятилетия назад.

Пороговые и предельные информационные ограничения являются всеобщими и проявляются не только в микромире или космофизике, но и в обычных масштабах. Поэтому, при определенных условиях и в обычных масштабах вполне можно ожидать проявления закономерностей явно не

классического характера, сходных с наблюдаемыми в микромире, в частности, может иметь место факт “параллелизма” виртуальных состояний.

До завершения анализа, проведенного в работе, намерено не было сказано ни одного слова об явных аналогиях с тем, что принято называть “квантовой” информацией [13]. Этим было продемонстрировано, что наличие виртуальных состояний объясняется существованием именно информационного порога (в любом, а не только в микро-масштабе). Второй целью анализа было показать, что “из-под порога” восприниматься может только шум (в том числе и в микромире), который не несет нам никаких сведений, кроме степени размытия классических состояний. Шум, приводящий к появлению совместных виртуальных состояний, по своим свойствам не является классическим [3,4], его характеристическим параметром является действие, а не энергия. Для описания поведения этого подпорогового шума (увеличения энтропии в условиях отсутствия классического шума), как раз и нужна дополнительная “квантовая” информация.

В квантовой механике постулируется так называемый акт измерения – считается, что под влиянием (?) измерительного прибора суперпозиционные состояния частиц переходят в классические. Однако, скорее имеет место не столько “влияние” измерительного прибора, сколько наличие у него порога восприятия. Это “влияние”, как показано во введении, имеется не только у прибора, но и у узкого потенциального барьера, который “не видит” частиц. Можно также говорить о носителях шума – виртуальных частицах, которые и порождают виртуальные состояния (для глаза, вооруженного микроскопом, это обычные молекулы жидкости). Конечно, виртуальные частицы в микромире имеют особенность, связанную с абсолютным минимумом константы действия – их нельзя зарегистрировать непосредственно, т.е. нельзя проверить их наличие экспериментально (в отличие от молекул, виртуальных только для глаза, хотя и вооруженного микроскопом). Таким образом, в поведении частиц в микромире не так уж много “странного” и необычного, если принять во внимание наличие информационного порога [3,4].

Существенным препятствием в построении даже отдельных вычислителей на основе виртуальных состояний, не говоря уже о компьютерах, реализующих алгоритмы по программе, включая алгоритмы с обратной связью (управление по данным), является именно случайность этих состояний, фактически приводящая к неуправляемости. Единственно, чем можно управлять, это значением вероятности их появления. Однако, вероятность достаточно точно определяется только на множестве событий (здесь имеется явное сходство с точным определением частоты – оно возможно только при большом числе колебаний). Поэтому говорить о скоростных вычислениях с использованием функций вероятности не приходится. Доступным практическому решению является только сравнительно небольшой класс задач, которые сводятся к нахождению максимума пика, либо периода повторения функции.

Регистр, построенный на разрядах, показанных на рис.6, является макро-устройством, действующим как виртуальный объект. Так же, как кубит он выдает при опросах все  $2^n$  состояний с теми или иными вероятностями.

## Литература

1. С.Г.Басиладзе. Информация как средство описания реальности, Препринт НИИЯФ МГУ № 2010-6/863, Москва 2010.
2. С.Г.Басиладзе. Пороговые и предельные информационные соотношения для сигналов. Препринт НИИЯФ МГУ- 2004-20/759, Москва 2004.
3. С.Г.Басиладзе. Пороговое и предельное информационные ограничения в динамике микромира. Препринт НИИЯФ МГУ-2007-13/834, Москва 2007.  
<http://dbserv.sinp.msu.ru:8080/sinp/files/pp-834.pdf>
4. С.Г.Басиладзе. Физика сигнала, Физика элементарных частиц и атомного ядра, Том 40, вып.6, Дубна 2009, с.1472÷1524.
5. А.Г.Алексенко, И.И.Шагурин. Микросхемотехника, Москва, Радио и Связь, 1982.
6. С.Г.Басиладзе. Пороговые ограничения, вносимые приемником в тракт передачи сигналов, Препринт НИИЯФ МГУ-2006-4/801, Москва 2006.
7. С.Г.Басиладзе. Физические особенности сложения и разложения сигналов и их информационные следствия, Препринт НИИЯФ МГУ-2006-2/801, Москва 2006.
8. Р.Фейнман. Моделирование физики на компьютерах, Квантовый компьютер и квантовые вычисления, “Регулярная и хаотическая механика”, Ижевск 1999, с.96.
9. Д.Дойч, Р.Джозса. Быстрое решение задач на основе квантовых вычислений, Квантовый компьютер и квантовые вычисления, “Регулярная и хаотическая механика”, Ижевск 1999, с.190.
10. П.Шор. Полиномиальные по времени алгоритмы разложения числа на простые множители и нахождения дискретного логарифма для квантового компьютера, Квантовый компьютер и квантовые вычисления, “Регулярная и хаотическая механика”, Ижевск 1999, с.200.
11. Lenstra A. K., Lenstra H. W., Lovász L. (1982). «Factoring polynomials with rational coefficients». *Math. Ann.* **261**.
12. E. Schrodinger, *Naturwissenschaften* **23** 807, 823, 844 (1935);  
Перевод на русский: Успехи химии, **5** 390 (1936);  
Перевод на английский: *Proc. Am. Philos. Soc.* 124 323 (1980).
13. С.А.Килин. Квантовая информация, Успехи физических наук, т.169 №5, 1999.
14. К.А.Валиев. Квантовые компьютеры и квантовые вычисления, Успехи физических наук, т.175 №1, 2005.
15. Nielsen M A, Chuang I L *Quantum Computation and Quantum Information* (Cambridge: Cambridge Univ. Press, 2000).

**Сергей Геннадьевич Басиладзе**

**Виртуальные состояния  
как следствие информационных ограничений,  
вычисления на основе виртуальных состояний**

Препринт НИИЯФ МГУ № 2011-3/867

Работа поступила в ОНТИ 09.06.2011 г