1 Порядок группы – число ее элементов. Порядок образующего элемента а циклической группы [a] – наименьшее n>0 такое, что an = 1. Группа G = (G, *, 1) наз. циклической. если (∃a Э G)(∃ n Э Z)(∀ x Э G)(x = a^n). Группа – моноид, каждый элемент которого обратим. Элемент называется обратимым, если (∃a’)a*a’=a’*a=ε – нейтральный элемент. (∀a)(a*ε=ε*a=a). Моноид – полугруппа с нейтральным элементом. Полугруппа – группоид с ассоциативной операцией ((a*b)*c=a*(b*c)). Группоид – алгебра с одной бинарной операцией G=(G, *). Полугруппу (в частности – группу) $(A,*)$ называют циклической, если существует такой элемент a, что любой элемент x полугруппы является некоторой целой степенью элемента a, который называют образующим элементом полугруппы (группы). Пример: полугруппа $(\mathbb{N},+)$ является циклической, образующий элемент: 1 (также бесконечная - $\forall n$ 1^n попарно различны). Возведение элемента a в положительную степень n есть сумма n этих элементов, что можно записать как n*a. Группа вычетов по модулю 3 $(\mathbb{Z}_3,+,0)$ также циклическая; любой ее ненулевой элемент является образующим. Группа называется конечной, если ее носитель – конечное множество. Порядок элемента a циклической группы – наименьшее положительное число n такое, что $a^n = 1$.
Теорема: Порядок образующего элемента конечной циклической группы равен порядку самой этой группы **Доказательство**: Пусть $(G,*,1)$ – конечная циклическая группа с образующим элементом a, n>0 – порядок этого элемента. Тогда все степени $a^0 = 1, a^1 = a, \dots a^{n-1}$ – попарно различны. Если бы $a^k = a^l, o < l < k < n$, то $a^{k-l} = a^{k+(-l)} = a^k a^{-l} = a^l a^{-l} = 1$ – существовала бы степень, меньшая n, при возведении в которую элемента a получится единица..
Для любого целого m существуют также целые n,k такие, что $m = kn + q$, где q – целое, $0 \le q < n$. Тогда $a^m = a^{kn+q} = a^{kn}a^q = (a^n)^k a^q = 1a^q = a^q \in \{1, a, \dots a^{n-1}\}$. Поскольку каждый элемент группы есть некоторая степень элемента a, то $G = \{1, a, \dots a^{n-1}\}$, порядок группы =n.

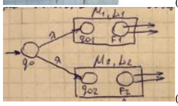
Формулы включения и исключения: Даны конечные множества $A_1 \dots A_n \subseteq U, n \ge 1$. Формула включения $|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n}[(-1)^{k+1}\sum_{i1<\dots<ik}|A_{i1} \cap \dots \cap A_{ik}|]$ Формула исключения: $|\overline{A_1 \cup \dots \cup A_n}| = |U| - \sum_{k=1}^{n}[(-1)^{k}\sum_{i1<\dots<ik}|A_{i1} \cap \dots \cap A_{ik}|]$ (формула исключения).

2 Поиск в глубину. На вход подается граф $G = (V, E)$, заданный списками смежности, и начальная вершина v0. На выходе имеем множества древесных и обратных ребер (T и B), множество F_c фундаментальных циклов, массив D, содержащий номера вершин. При достижении некоторой вершины v (при запуске алгоритма v=v0), с неё снимается метка «новая», ей присваивается D-номер, вершина v заносится в стек и просматриваются вершины из её списка смежности $L[v]$. | В случае ориентированного графа, в результате поиска в глубину получают также множество прямых дуг $F = \{(u,v): D[u] < D[v],\ v \notin Stack\}$, ведущих от подлинного предка к подлинному потомку в глубинном остовном лесу; обратных дуг $B = \{(u,v): D[u] \ge D[v],\ v \in Stack\}$, ведущих от потомков к предкам (в том числе петли); поперечных дуг $C = \{(u,v): D[u] > D[v],\ v \notin Stack\}$, не являющихся ни древесными, ни прямыми, ни обратными. Орграф бесконтурен тогда и только тогда, когда при поиске в глубину (независимо от выбора начальной вершины) множество обратных дуг пусто. | Древесная дуга – ведет от отца к сыну в глубинном остовном лесу. Прямая дуга – ведет от подлинного предка к подлинному потомку. Обратная дуга – от потомков к предкам (включая петли). Поперечная – не древесная, не пряма, не обратная.. Глубинный остовный лес – макс. остовный лес, находимый поиском в глубину.

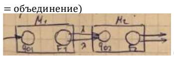
```
T,B,FC,Stack:=0; Count := 1
For all v∈V do New[v] := 1 end
For all v∈V while (∃v)(New[v] = 1) do
  Search_D(v) end
End
Proc Search_D(v)
New[v] := 0
D[v] := Count;  Count := Count + 1
v -> Stack
For all (w ∈ L[v]) do
 If New[w] then begin
.   {v,w} → T
.   Search_D(w)
. End if
. Else
.   if {v,w} ∉ T then begin
.     {v,w} → B
.     Read(v..w) → Fc
.   end if
End for
Stack → v
End Search_D
```

Язык регулярен тогда и только тогда, когда он допускается КА (язык L является элементом полукольца R).Теорема Клини: язык регулярен ⇔ он допускается некоторым КА. Алгоритм синтеза КА по рег. выражениям: (для любого регулярного языка может быть построен КА, его допускающий)

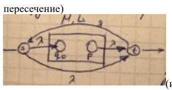
(КА для простейших регулярных языков)



(F=F₁ ∪F₂, L₁∪L₂, параллельное соединение = объединение)



(F = F₂, L1*L2, последовательное соединение - пересечение)



(итерация L*, если перерубить нижнюю дугу, то L^+=L*L=LL* - положительная итерация)

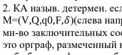
3 Индуктивное упорядоченное множество. Теорема о неподвижной точке
Упорядоченное множество $\mathcal{A}$ называется индуктивно упорядоченным, если в нем есть наименьший элемент, а любая неубывающая последовательность элементов $\{a_n\}_{n\ge0}$ имеет точную верхнюю грань. Элемент aЭA наз. наим. [наиб.], если (∀x Э A)(x>=a)[x<=a]. Элемент наз. мин. [макс], если ∀(x)(x<=a)[x>=a]. Элемент наз. верх. [нижн.] грань подмножества B, если (∀xЭB)(x<=a)[x>=a]. Наименьший элемент из множества всех верхних граней наз. точной верхней гранью. Пусть $(A,\le), (B,\preccurlyeq)$ – индуктивные упорядоченные множества. Отображение $f: A \to B$ называется непрерывным, если справедливо равенство $f(\sup a_n) = \sup f(a_n)$. Элемент $a \in A$ называют неподвижной точкой отображения $f: A \to A$, если $f(a) = a$. Элемент a называют наименьшей неподвижной точкой отображения, если он является наименьшим элементом множества всех неподвижных точек отображения.
Теорема: любое непрерывное отображение f индуктивно упорядоченного множества $(M,\le)$ $f: M \to M$ имеет наименьшую неподвижную точку. **Доказательство:** Пусть $\mathbb{O}$ – наименьший элемент ИндуктивноУпорядоченногоМножества M. Построим последовательность $\{\mathbb{O}, f(\mathbb{O}), f(f(\mathbb{O})), \dots f^n(\mathbb{O}), \dots\}$, где $f^n(x) = f(f^{n-1}(x))$. Т.к. $\mathbb{O}$ – наименьший элемент, то $\mathbb{O} \le f(\mathbb{O})$, т.е. при n=0 $f^n(\mathbb{O}) \le f^{n+1}(\mathbb{O})$. Пусть $f^n(\mathbb{O}) \le f^{n+1}(\mathbb{O})$ $\forall n \le k$. $f^{k+1}(\mathbb{O}) = f(f^k(\mathbb{O})) \le f(f^{k+1}(\mathbb{O}))$, следовательно, $f^{k+1} \le f^{k+2}(\mathbb{O})$, т.е. последовательность не убывает. Обозначим $a = \sup f^n(\mathbb{O})$, $n \ge 0$. Тогда $f(a) = f(\sup f^n(\mathbb{O})) = \underset{n\ge0}{\sup}(f^{n+1}(\mathbb{O})) = \underset{n\ge1}{\sup} f^n(\mathbb{O}) = a$. Таким образом, f(a)=a, т.е. a – неподвижная точка. Пусть теперь f(b)=b. $\mathbb{O} \le b$, $\Rightarrow f(\mathbb{O}) \le f(b) = b$, $f(f(\mathbb{O})) \le f(f(b)) = b, \dots$. $(\forall n \ge 0)$ $(f^n(\mathbb{O}) \le b)$ – значит b является верхней гранью последовательности $\{f^n(\mathbb{O})\}_{n\ge0}$. Однако a – ТОЧНАЯ верхняя грань этой последовательности, поэтому $a \le b$.

```
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    d := M[v]+φ(v,w)
    If d < M[w] then begin
      M[w] := d
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
Волнового фронта (когда вес всех дуг =1)
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    If M[W]=+∞ then begin
M[W]:=M[V]+1
W->Q
end
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
```

4 Кольца. Аддитивная группа и мультипликативный моноид кольца. Теорема о тождествах кольца. Кольцом называют алгебру вида $(R,+,*,0,1)$, сигнатура которой состоит из двух бинарных (сложение кольца и умножение кольца) и двух нульарных операций, причем для любых $a,b,c \in R$ выполняются равенства, называемые аксиомами кольца:1)$a+(b+c) = (a+b)+c$; 2)$a+b = b+a$; 3)$a+0 = a$; 4)$\forall a \in R\ \exists(-a)$: $a+(-a) = 0$; 5)$a*(b*c) = (a*b)*c$; 6)$a*1 = 1*a = 1$; 7)$a*(b+c) = a*b+a*c$; $(b+c)*a = b*a+c*a$; | Аксиомы 1-4 означают, что алгебра (R,+,0) является абелевой (коммутативной) группой, называемой аддитивной группой кольца. Аксиомы 5 и 6 показывают, что алгебра (R,*,1) является моноидом, называемым мультипликативным моноидом кольца. | Кольцо называется коммутативным, если его операция умножения коммутативна. | Кольцо (коммутативное) вычетов по модулю k – алгебра вида $Z_k = (\{0,1,\dots,k-1\}, \oplus_k, \odot_k, 0, 1)$ с операциями сложения по модулю к и умножения по модулю к.
Теорема: в любом кольце выполняются следующие тождества:1) $0*a = a*0 = 0$; 2)$(-a)*b = -(a*b) = a*(-b)$; 3) $(a-b)*c = a*c-b*c$; $c*(a-b) = c*a-c*b$;**Доказательство**: 1) для произвольного a, $a+0a = 1a+0a = (1+0)a = 1a = a$. $a+0a = a$ можно рассматривать как уравнение относительно неизвестного 0a: $0a = a-a = 0$. Тождество a0=0 доказывается аналогично; 2) Докажем $-(ab) = a(-b)$: $a(-b)+ab = a((-b)+b) = a0 = 0$. Отсюда $a(-b) = -(ab)$. Аналогично доказывается$(-a)b = -(ab)$; 3) Рассмотрим $(a-b)c = ac-bc$. С учетом доказанного выше, $a(b-c) = a(b+(-c)) = ab+a(-c) = ab-ac$. Второе тождество доказывается аналогично.
Для любого КА может быть построен эквивал. ему детерминированный КА. КА называют детерминированным, если: в нем нет λ -переходов, и из каждого состояния по любому символу возможен переход только в одно состояние. КА M1 и M2 называют эквивалентными, если они допускают один и тот же язык.
Для любого конечного автомата может быть построен эквивалентный ему детерминированный КА. Детерминизация происходит в два этапа – на первом происходит удаление из автомата лямбда-переходов, на втором непосредственно детерминизация (например с помощью метода вытягивания).
Если дан КА $M = (V,Q,q_0,F,\delta)$без λ -переходов, то детерминированный $M' = (V,Q',q_0',F',\delta')$, где $Q' = 2^Q, q_0' = \{q_0\}$, $F' = \{T: T \cap F = \emptyset\}$, $\delta'(S,a) = \bigcup_{q\in S}\delta(q,a)$.
В свою очередь, для любого детерминированного КА может быть построен эквивалентный ему детерминированный КА с минимальным числом состояний. Минимизация происходит за счет «группировки» состояний в классы эквивалентности. Пусть даны два регулярных языка L1 и L2. Тогда регулярными языками также будут их дополнения ($\bar{L} = V^*/L$), пересечение $(L1 \cap L2 = \overline{\overline{L1} \cup \overline{L2}})$, разность $(L1/L2 = L1 \cap \overline{L2})$ и симметрическая разность $(L1\Delta L2 = (L1/L2) \cup (L2/L1))$ Проблема пустоты: дан КА, необходимо выяснить, не является ли пустым язык, который он допускает. Проблема эквивалентности: для двух заданных КА M1 и M2 необходимо проверить, являются ли они эквивалентными, т.е. совпадают дли допускемые ими языки.

5 Область целостности. Теорема о конечной области целостности. Поля вычертов.
Область целостности – коммутативное кольцо без делителей нуля. Ненулевые элементы a и b кольца R – делители нуля, если a*b = 0(b*a=0). Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют *телом*; коммутативное тело – *полем*. (Поле – конечная область целостности) В поле, помимо аксиом кольца, выполняются еще два тождества: $\forall a \ne 0 \in R,\ \exists a^{-1}$: $a*a^{-1} = 1$; $a*b = b*a$. | Ненулевые элементы a,b кольца R называют делителями нуля, если $a*b = 0$ или $b*a = 0$. Областью целостности называется коммутативное кольцо без делителей нуля (к примеру, кольцо целых чисел).
Иньъекция – отображение, каждый элемент из R(f) имеет единственный прообраз из f(x1)=f(x2)=>x1=x2; Сюръекция – отображение f:A->R R(f)=B (∀y Э B)(∃x Э A)(y=f(x)); Биекция – оба (∀y Э B)(∃ !x Э A)(y=f(x)) | **Теорема:** Конечная область целостности является полем. **Доказательство:** Поле – кольцо, умножение которого коммутативно, а каждый ненулевой элемент имеет обратный элемент относительно умножения. Так как по определению область целости является коммутативным кольцом, то достаточно доказать, что для конечной области целостности любой ненулевой элемент обратим. Фиксируем произвольный $a \ne 0$ и определим отображение f_a множества всех ненулевых элементов в себя: $f_a(x) = a*x$. Это отображение будет инъекцией – из равенства $a*x = a*y$ следует $a*(x-y) = 0$; ввиду отсутствия делителей нуля получаем что $x-y = 0$; $x = y$. Так как носитель по условию теоремы конечен, то f_a будет также и биекцией. Поэтому для любого y существует единственный элемент x, такой, что $y = a*x$. При $y = 1$ равенство $a*x = 1$ выполняется для некоторого однозначно определенного $x = a^{-1}$.
Кольцо вычетов по модулю p $\mathbb{Z}_p$ является полем тогда и только тогда, когда p – простое число.
Рекуррентным соотношением k-го порядка называется последовательность $(\mathbf{0})$ $x_n = \phi(x_{n-1}, x_{n-2}, \dots, x_{n-k}\} + f(n)$. Порядок указывает, от скольких предыдущих членов зависит n-й член последовательности. При $f(n) \equiv 0$ рекуррент называется однородным. Если ф – линейна по аргументам, т.е. $(\mathbf{1})$ $x_n = a_1(n)x_{n-1} + \dots + a_k(n)x_{n-k}$, то соотношение называется линейным. Если $a_i = const$, то ЛРС $(\mathbf{2})$ $x_n = a_1x_{n-1} + \dots + a_kx_{n-k}$ называется ЛРС с постоянными коэффициентами.
Решить РС в общем случае – найти такую последовательность {yn} (частное решение), что будучи подставленной в (1) yn обращает его в тождество. Решение ЛРС (2) должно быть дополнено начальными условиями $(\mathbf{3})$ $x_i = \alpha_i$, $i = \overline{0, k-1}$. **k** линейно независимых решений ЛРС **k**-го порядка образуют фундаментальную систему решений этого ЛРС. **Теорема**: Пусть $\{y_n^{(1)}\} \dots \{y_n^{(k)}\}$ – ЛНЗ решения соотношения $x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = 0$. Тогда любое его решение можно представить в виде их линейной комбинации для некоторых констант C.
Доказательство: Задав некоторые начальные условия, покажем что константы C задаются однозначно. Запишем начальные условия для линейной комбинации $(\mathbf{1})\begin{cases} \sum_{i=1}^{k} C_i y_0^{(i)} = \alpha_0 \\ \sum_{i=1}^{k} C_i y_1^{(i)} = \alpha_1 \\ \dots \\ \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = \alpha_{k-1} \end{cases}$. Для системы (1) Δ= $\begin{bmatrix} y_0^{(1)} & \cdots & y_0^{(k)} \\ \vdots & \ddots & \vdots \\ y_{k-1}^{(1)} & \cdots & y_{k-1}^{(k)} \end{bmatrix}$. Предположим, что Δ= 0 – тогда однородная система $(\mathbf{2})$ $\sum_{i=1}^{k} C_i y_j^{(i)} = 0$ соответствующая системе (1) имеет тривиальное решение. В этом случае из (2) можно найти (не все равные нулю) константы C. Однако (2) также определяет решение, соответствующее *нулевым начальным условиям*, следовательно, $\sum_{i=1}^{k} C_i y_n^{(i)} \equiv 0$. Возникает противоречие, следовательно Δ≠ 0, а (1) имеет единственное решение. Таким образом, начальные условия задают однозначный набор C, т.е. любое решение (1) можно определить в виде ЛК фундаментальных

61. Полукольцо – алгебра с двумя бинарными и двумя нульарными операциями S_M=(S,+,*,0,1). (отличие полукольца от кольца – в ней нет вычитания и обратных элементов). Аксиомы полукольцац:1) (a+б)+c=a+(б+c); 2) a + б = б + a; 3) a + 0 = a; 4) (a*б)*c=a*(б*c); 5) a *1=1*a=a; 6) a(б+c)=aб+бc; 7) (б+c)a=бa+ca; 8) аннулирующее св-во нуля: a*0=0*a=0; Частные случаи полукольца: 1) коммутативное полукольцо (aб=бa); 2) идемпотентное полукольцо: a+a=a; Замкнутое полукольцо – 1) любая последовательность элементов имеет точную верхнюю грань по естественному порядку; 2) (∀a ϵS) и (∀$\{b_n\}_{n>=0}$) a sup bn=sup(abn); sup(bn)a=sup(bna) ; Операция умножения непрерывна по опр.. Обычная непрерывность: f(∑ x_n)= ∑f(x_n). Непрерывность сложения: a+∑(x_n)= ∑ (a+x_n). (выполняется для любой последовательности замкн. Полукольца и любого эл-та этого полукольца). ТЕОРЕМА: Наименьшими решениями уравнений x=ax+б (1) и x=xa+б (2) будут соответственно: x=a*б и x=бa* (* - итерация). *Док-во:* в инд. Уп. Мн. Определено наименьшее решение уравнения x=f(x), где f непрерывна.По теореме о неподвижной точке выведем формулу наименьшего решения уравн. 1.: x_0=supf*(0), где 0 – наим. Эл-т и.у.м..Для замкн. Полукольца получим: x_0=sup{0, b, ab+b=b(a+1),a(ab+b)+b=(a^2+a+1)b,…,(1+a+…+a^n)b,…}=$\sum_0^\infty$[(1+a+…+a^n)b]= $\sum_0^\infty$[(1+a+…+a^n)]b=$\sum_0^\infty$[a^n]b; $\sum_0^\infty$[a^n]=a* - итерация. Второе доказывается аналогично, ***чтд***. В полукольце с тривиальной итерацией ∀a: a*=1, x0=б. Индуктивно упорядоченное множество – это мн-во, кот. Имеет наим. Эл-т и любая неуб. Посл-ть кот-ого имеет точную верхн. Грань. Теорема о неподвижн. Точке: всякое непрерывн. Отображение и.у.мн. в себя имеет наименьшую неподвижную точку.
2. КА назыв. детермен. если 1) в нем нет лямбда перех. 2)(∀qϵQ) (aϵV) (δ(q,a)=1). КА M=(V,Q,q0,F,δ)(слева направо:алфавит, мн-во состояний КА, начальное состояние, мн-во заключительных сост., функции перехода).Состояния – это вершины КА.КА-это орграф, размеченный над полукольцом регулярных языков, так что вес равен либо букве алфавита, либо лямбде. Теорема: Для любого КА может быть построен эквивалентный ему детерменированный КА. Док-во – алгоритм построения детерм. КА без лямбда-переходов. 1)удаление лямбда-переходов. Дан КА M=(V,Q,q0,F,δ), строим M’=(V,Q’,q0’,F’,δ’).Q’={q0}U{p:(∃qϵQ) (∃aϵV)(q->$_a$p)}.q0’=q0.F’=(F⋂ Q')U(q:q=>$^*\gamma$fϵF)



Остаются все дуги исх. Автомата, не явл. Лямбда переходами. 2) Детерминизация. Исходный КА M = (Q,E, q0,F, δ) – без λ-переходов Строим КА M’ = (Q’,E’, q’0,F’, δ’). Q’ = 2Q ; q0’ = {q0}; F’ = {T: T F ≠ ∅} δ’(S,a) = U(q∈S) δ(q,a)

7 1. Пусть $\mathcal{G} = (G,*,1)$ – группа, $\mathcal{H} = (H,*,1)$ – ее подгруппа. Левым смежным классом подгруппы $\mathcal{H}$ по элементу $a \in G$ называют множество $aH = \{y:\ y = a*h, h \in H\}$.; правым смежным классом – множество $Ha = \{y:\ y = h*a, h \in H\}$.
Теорема Лагранжа: порядок конечной группы делится на порядок любой ее подгруппы. Доказательство: пусть любая группа μ = (G, *, 1) и H = (H, *, 1) – какая-то ее подгруппа. Пусть a ∈ G (не обязательно a ∈ H). Левый (правый) смежный класс подгруппы H по эл. a: aH ⇔ {ah: h ∈ H} (Ha ⇔ {ha: h ∈ H })
Лемма 1:{∀hϵH: hH=H}; Лемма 2: ($\forall a, b\epsilon G$) a(bH)=abH; Лемма 3: левые смежные классы попарно не пересекаются и образуют разбиение группы. Лемма 4: все левые сежные классы находятся между собой во взаимно однозн. Соотв-ии.Все 4 леммы справедливы для любой группы. |H|=|aH| для любого aϵG.Попарно эквивалентны->все мн-ва состоят из одного и того же числа эл-ов.|G|-порядок группы, k-число смежных классов, индекс подгруппы в группе, |H| - порядок группы. |G|*k= |H|.Итак, для любой конечной группы ее порядок (число ее эл-ов) пропорционален порядку любой ее подгруппы, т.е. делится на него.***чтд***
2. Размеченным ориентированным графом называют пару $W = (G, \phi)$, где $G = (V, E)$ – обычный ориентированный граф, $\phi: E \to S/\{0\}$ – функция разметки со значениями в некотором идемпотентном полукольце $\mathcal{S} = (S,+,*,\mathbb{O},\mathbf{1})$, $(\forall e \in E)(\phi(e) \ne \mathbb{O})$.
Если задать орграф с помощью матрицы смежности $A = \left(a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ \mathbb{O}, & \text{иначе} \end{cases}\right)$, то задача о достижимости сводится к вычислению матрицы достижимости графа $C = \left(c_{ij} = \begin{cases} 1, & v_i \to^* v_j \\ \mathbb{O}, & \text{иначе} \end{cases}\right)$.Если задать орграф с помощью матрицы меток дуг $A = \left(a_{ij} = \begin{cases} \phi(v_i, v_j), (v_i, v_j) \in E \\ \mathbb{O}, \text{иначе} \end{cases}\right)$, то задача о поиске кратчайших расстояний между двумя узлами графа сводится к вычислению матрицы кратчайших расстояний $C = \left(c_{ij} = \begin{cases} \text{длине кратчайшего пути из } v_i \text{в } v_j, \text{если } v_i \Rightarrow^* v_j \\ +\infty, \text{иначе} \end{cases}\right)$. Обе задачи можно решить с помощью алгоритма Флойда – Уоршелла – Клини. В случае задачи о достижимости, в качестве полукольца $\mathcal{S}$ выбирают полукольцо $\mathbb{B} = (\{0,1\}, max, min, 0, 1)$, а в случае задачи о поиске кратчайших расстояний: $\mathcal{R}^+ = ([0,+\infty], min, +, +\infty, 0)$. Метка пути W: φ*(W)={1, если |W|=0; φ(l1)* φ(l2)*…* φ(lm), если W=|m|>0. L – вес дуг. Стоимость прохождения из Vi -> Vj: C=C(Vi,Vj)=∑ φ*(W) (под фи-W:Vi=>*Vj)
Лемма 1: (∀hϵH)hH=H
Док: Пусть x∈ hH,т.е. x=h*h1, h1∈ H=>x∈ H. Обратно: если x∈ H,то x=h(h^-1*x)=x, но h, $h^{-1}, x \in H$=>x∈ hH. Следн-но hH=H.
Лемма 2: $(\forall a, b \in G)$ $a(bH) = abH$.
Док следует из ассоциативности групповой операции.
Лемма 3: Левые смежные классы попарно не пересекаются и образуют разбиение группы.
Док: Пусть aH≠ bH и aH∩ $bH \ne \emptyset$,т.е. сущ. Z∈ $aH \cap bH$. Тогда z=ah1=bh2, h1,h2∈ H, имеем ah1=bh2=>b=ah1$h2^{-1}$. Тогда bH= (ah1$h2^{-1}$)H= ah1$(h2^{-1}H) = ah1H = aH$. -противоречие=>Классы не пересекаются. $(\forall x \in H)$(x=x*1∈ xH), т. к. 1 ∈ H =>каждый эл-т принадлежит какому-либо классу(образует разбиение)
Лемма 4: Все левые смеж. Классы наход. Между собой во взаимно одназнач. Соотв.
Док: установим взамн.од.соотв. между подгр. H и произвольным лев. Симм. Классом по эл-ту не принадлежащему продгр. φ:H→aH, a не∈H,где. φ(H) = ah, h∈ H.
φ – сюрьекция, т. к. , если x∈ aH, То x=ah, h∈ H, откуда x= $\varphi(h)$.
φ – иньъекция,т.к. $\varphi(h1) = \varphi(h2)$=>ah1=ah2=>h1=h2. Отсюда φ – биекция.

8

```
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    d := M[v]+φ(v,w)
    If d < M[w] then begin
      M[w] := d
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
Волнового фронта (когда вес всех дуг =1)
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    If M[W]=+∞ then begin
M[W]:=M[V]+1
W->Q
end
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
```

Неоднородным ЛРС с постоянными коэффициентами называют ЛРС вида $(\mathbf{1})$ $x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = f(n)$, a=const. **Теорема**: Общее решение соотношения (1) есть сумма общего решения соответствующего ему однородного ЛРС $x_n + a_1x_{n-1} + \dots + a_kx_{n-k} = 0$ и частного решения неоднородного ЛРС (1).**Доказательство**: пусть Y_n – какое-то частное решение (1). Тогда $(\mathbf{2})$ $x_n^{он} = Y_n + \sum_{i=1}^{k} C_i y_n^{(i)}$, где $\{y_n^{(1)} \dots y_n^{(k)}\}$ – ФСР соответствующего ОЛРС. Зададим произвольные начальные условия, $y_o = \alpha_0, \dots y_{k-1} = \alpha_{k-1}$, которым соответствует решение y_n, ⇒
$(\mathbf{3})\begin{cases} Y_0 + \sum_{i=1}^{k} C_i y_0^{(i)} = \alpha_0 \\ Y_1 + \sum_{i=1}^{k} C_i y_1^{(i)} = \alpha_1 \\ \dots \\ Y_{k-1} + \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = \alpha_{k-1} \end{cases} \Rightarrow (\mathbf{4})\begin{cases} \sum_{i=1}^{k} C_i y_0^{(i)} = \alpha_0 - Y_0 \\ \sum_{i=1}^{k} C_i y_1^{(i)} = \alpha_1 - Y_1 \\ \dots \\ \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = \alpha_{k-1} - Y_{k-1} \end{cases}$. Для системы (4) Δ= $\begin{bmatrix} y_0^{(1)} & \cdots & y_0^{(k)} \\ \vdots & \ddots & \vdots \\ y_{k-1}^{(1)} & \cdots & y_{k-1}^{(k)} \end{bmatrix}$. Предположим, что Δ= 0 – тогда однородная система $(\mathbf{5})\begin{cases} \sum_{i=1}^{k} C_i y_0^{(i)} = 0 \\ \sum_{i=1}^{k} C_i y_1^{(i)} = 0 \\ \dots \\ \sum_{i=1}^{k} C_i y_{k-1}^{(i)} = 0 \end{cases}$ соответствующая системе (4) имеет тривиальное решение. В этом случае из (5) можно найти (не все равные нулю) константы C. Однако (5) также определяет решение, соответствующее *нулевым начальным условиям*, следовательно, $\sum_{i=1}^{k} C_i y_n^{(i)} \equiv 0$. Возникает противоречие, следовательно Δ≠ 0, а (4) имеет единственное решение. Таким образом, начальные условия задают однозначный набор C, т.е. любое регение (1) можно определить в виде (2). Частное решение неоднородного ЛРС находится методом подбора. Если $f(n) = a^n P^{(m)}(n)$, то $x_n^{чн} = n^s a^n Q^{(m)}(n)$, где Q – полином с неопределенными коэффициентами, которые могут быть определены путем подстановки в соотношение, s – кратность корня a характеристического уравнения (если a не является корнем, то s=0). Если $f(n) = a^n[P^{(m)}(n)\cos n\phi + Q^{(l)}(n)\sin n\phi]$, то $x_n^{чн} = n^s a^n[P^{(p)}(n)\cos n\phi + Q^{(p)}(n)\sin n\phi]$, где s – кратность корня $ae^{i\phi}$ характеристического уравнения, $p = \max m, l$. **Принцип суперпозиции**: Пусть в неоднородном ЛРС (1) $f(n) = \sum_{i=1}^{m} g_i(n)$ – сумма последовательностей, и пусть $x_n^{чн_i}$ есть решение соотношения (1) при $f(n) = g_i(n)$. Тогда частное решение $x_n^{чн} = \sum_{i=1}^{m} x_n^{чн_i}$.

9

```
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    d := M[v]+φ(v,w)
    If d < M[w] then begin
      M[w] := d
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
Волнового фронта (когда вес всех дуг =1)
For all v∈V do M[v] := +∞ end
v0→Q;
M[v0]=0
For all v∈Q while Q≠0 do
  For all w∈p[v] do
    If M[W]=+∞ then begin
M[W]:=M[V]+1
W->Q
end
    If w ∉Q then w->Q
    End if
  End for
Q->v
Endfor
```

Теорема: Если L – регулярный язык, то существует натуральная константа K_L, зависящая от L, такая, что для любой цепочки $x \in L$, длина которой не меньше K_L, x допускает представление в виде $x = uvw$, где $v \ne \lambda$ и $|v| \le K_L$. При этом для любого $n \ge 0$ существует цепочка $x_n = uv^nw \in L$. **Доказательство**: Т.к. L – РЯ, его допускает некий детерминированный КА $M = (V, Q, q_0, F, \delta)$. Пусть $K_L = |Q|, x \in L, |x| \ge K_L$. Значит, цепочка читается на единственном пути длины $m = |x| \ge |Q|$. Значит, число вершин в пути больше числа дуг, а следовательно, путь можно разбить на три части: $\to q_0 \leadsto_u p \circlearrowleft_v p \leadsto_w p_m \to$. Тогда $(\forall n \ge 0)(uv^nw \in L)$; т.к. контур – простой путь длины≠ 0, то $0 < |v| \le K_L$.

10 Размеченным (взвешенным) ориентированным графом называют пару $W = (G, \phi)$, где $G = (V, E)$ – обычный ориентированный граф, $\phi: E \to \mathcal{R}$ – функция разметки со значениями в некотором идемпотентном полукольце $\mathcal{S} = (S, +, *, \mathbb{O}, \mathbf{1})$, $(\forall e \in E)(\phi(e) \neq \mathbb{O})$. Если задать орграф с помощью матрицы смежности $A = \left(a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ \mathbb{O}, & \text{иначе} \end{cases}\right)$, то задача о достижимости сводится к вычислению матрицы достижимости графа $C = \left(c_{ij} = \begin{cases} 1, & v_i \to^* v_j \\ \mathbb{O}, & \text{иначе} \end{cases}\right)$. Если задать орграф с помощью матрицы меток дуг $A = \left(a_{ij} = \begin{cases} \phi(v_i, v_j), & (v_i, v_j) \in E \\ \mathbb{O}, & \text{иначе} \end{cases}\right)$, то задача о поиске кратчайших расстояний между двумя узлами графа сводится к вычислению матрицы кратчайших расстояний $C = \left(c_{ij} = \begin{cases} \text{длине кратчайшего пути из } v_i \text{в } v_j, & \text{если } v_i \Rightarrow^* v_j \\ +\infty, & \text{иначе} \end{cases}\right)$. Обе задачи можно решить с помощью алгоритма Флойда – Уоршелла – Клини. В случае задачи о достижимости, в качестве полукольца $\mathcal{S}$ выбирают полукольцо $\mathbb{B} = (\{0,1\}, max, min, 0,1)$, а в случае задачи о поиске кратчайших расстояний: $\mathcal{R}^+ = ([0, +\infty], min, +, +\infty, 0)$. После этого матрица $C = A^*$ находится путем ерешения системы уравнений $\xi = A\xi + \varepsilon_j$, где $\varepsilon_j \in \mathcal{R}^n$ – j-й вектор единичной матрицы в полукольце B или R+. Наименьшее решение имеет вид $\xi = A^* \varepsilon_j$, тогда столбцы ξ есть j-е столбцы матрицы C.

Говорят, что группа G действует слева на множестве M, если задан гомоморфизм $\phi: G \to S(M)$ из группы G в симметрическую группу S(M) множества M, т.е. на симметрической группе множества задано множество подстановок. Пусть $A = \{a_1 \dots a_n\}$ – множество, $G \subseteq S_n$ – подгруппа циклической группы этого множества. Элементы $a, b \in A$ называют эквивалентными $a \sim b$, если $b = \sigma(a), \sigma \in G$. Орбитой элемента a называют его класс эквивалентности $[a]_\sim$ по подстановке σ. Стабилизатором элемента $s \in A$ называют множество $G_s = \{\sigma : \sigma(s) = s\}$.

Лемма Бернсайда: Число N орбит множества S равно $N = \frac{1}{|G|} \sum_{s \in S} |G_s|$.

(Доказательство только на «5», вроде)

11 Пусть H – некая конечная группа, являющаяся подгруппой группы подстановок Sn. Произвольную подстановку $h \in H$ можно представить в виде произведения независимых циклов $h = c_1 \circ \dots \circ c_m$, $m \leq n$. Цикловым индексом группы H называется многочлен $p_H(x_1, \dots, x_n) = \frac{1}{|H|} \sum_{h \in H} t_\sigma$, где $t_\sigma = x_1^{l_1} \dots x_k^{l_k}$ – мультипликативный терм, li – число циклов длины I в разложении элемента на независимые циклы.**Теорема Пойа:** пусть $S = \{1..n\}$ – множество, на котором действует группа G, $R = \{r_1, \dots, r_m\}$ – множество цветов, $p_{G(x_1, \dots, x_n)}$ – цикловой индекс группы G. Тогда:1) перечень классов эквивалентности можно представить в виде $Invt(R^S/\sim) = p_G(\sum_{r \in R} w(r), \dots, \sum_{r \in R} w^n(r))$ 2) число неэквивалентных раскрасок из {R} множества $N = P_G(|R|, \dots, |R|)$. **Доказательство** второго утверждения: по лемме Бернсайда, $N = \frac{1}{|G|} \sum_{s \in S} |G_s| = \frac{1}{|G|} \sum_{\sigma \in G} \psi(\sigma)$, где $\psi(\sigma)$ – число всех элементов s, остающихся неподвижными в результате действия подстановки σ. Подстановка $\sigma = c_1 c_2 \dots c_{l = K(\sigma)}$ представлена в виде m независимых циклов. Чтобы циклы сохраняли разметку, элементы должны быть покрашены одинаково. Вычислим терм $\hat{t}_\sigma = (w_1 + \dots + w_m)^{l1} (w_1^2 + \dots + w_m^2)^{l2} \dots (w_1^n + \dots + w_m^n)^{ln}$. Циклический индекс группы G $P_G(x_1 \dots x_n) = \frac{1}{|G|} \sum_{h \in H} t_\sigma = \frac{1}{|G|} \sum_{h \in H} x_1^{l_1} \dots x_k^{l_k}$. Тогда, $\hat{t}_\sigma = t_\sigma |_{x_k = (w_1^k + \dots + w_m^k)}$. $\psi(\sigma) = |R|^{K(\sigma)}$; $l_1 + \dots + l_n = K(\sigma) \Rightarrow \psi(\sigma) = \widehat{t_\sigma}|_{\forall w_i\, w_i = 1} = \widehat{t_\sigma}|_{\forall i\, x_i = m}$. Поэтому само число классов эквивалентности $N = \frac{1}{|G|} \sum_{\sigma \in G} t_\sigma |_{x_i = m} = P_G(x_1 \dots x_m)|_{x_i = m} = P_G(m \dots m)$.

Непрерывность операции сложения в замкнутом полукольце. Теорема о наименьшем решении линейного уравнения в замкнутом полукольце. Полукольцо — это алгебра с двумя бинарными и двумя нульарными операциями S=(S,+,·,0,1), такая, что для произвольных элементов a,b,c множества S выполняются следующие равенства, называемые аксиомами полукольца: 1)a+(b+c)=(a+b)+c; 2)a+b=b+a; 3)a+0=a; 4)a·(b·c)=(a·b)·c; 5)a·1=1·a=a; 6)a·(b+c)=a·b+a·c; 7)(b+c)·a=b·a+c·a; 8)a·0=0·a=0. Для любой последовательности $\{x_n\}_{n \in \mathbb{N}}$ элементов замкнутого полукольца и любого элемента a этого полукольца выполняется равенство $a + \sum x_n = \sum (a + x_n)$ – операция сложения в замкнутом полукольце непрерывна. **Теорема:** Наименьшими решениями уравнений $x = ax + b$ и $x = xa + b$ в замкнутых полукольцах являются соответственно $x = a^* b$ и $x = b a^*$; a* - итерация элемента a.

Доказательство: Для случая x=ax+b, $x = \sum_{n \geq 0}^{\infty} f^n(0)$, где 0 – нуль полукольца, f(x)=ax+b. $f^0(0) = 0, f^1(0) = b, f^2(0) = (a+1)b, \dots, f^n(0) = (a^{n-1} + \dots + a + 1)b$. Получаем, что $\sum_{n=0}^{\infty} f^n(0) = \sum_{n=1}^{\infty} [(a^{n-1} + \dots + a + 1)b] = [\sum_{n=1}^{\infty} (a^{n-1} + \dots + a + 1)] * b$. $\sum_{n=1}^{\infty} (a^{n-1} + \dots + a + 1) = \sum_{n=1}^{\infty} a^n = a^*$, т.е. в итоге получаем что $x = \sum_{n=1}^{\infty} f^n = a^* b$.