№1.

Пусть f – односторонняя и вычислима за $p(n)$, $n = |x|$

Тогда $\tilde{f}(a, x) = a f(x)$, где $|a| = p(n)$ – вычислима за линию

Допустим, умеем хорошо обращать $\tilde{f}(a, x)$, тогда умеем и $f(x)$ – допишем случайное a перед $f(x)$, обратим и возьмем x из полученной пары (a, x) после обращения, значит $f(x)$ – не односторонняя, противоречие. Значит, $\tilde{f}(a, x)$ – односторонняя и ~~ра~~ вычислимая за линию.

Занумеруем все машины Тьюринга, пусть $M_{\tilde{f}}$ – номер машины, которая вычисляет $\tilde{f}$ – одностороннюю функцию, вычислимую за линию. Пусть $g_n(x_1, \dots x_n) = M_1(x_1) M_2(x_2) \dots M_n(x_n)$, где $M_i(x_i)$ – результат работы M_i на x_i через $|x_i|$ шагов. Тогда, если $\exists$ односторонняя f, то $\exists$ и $\tilde{f}$, тогда $\exists\, n_0$: g_{n_0} содержит результат $\tilde{f}(x)$ ($n_0 = M_{\tilde{f}}$). Тогда, если g_{n_0} – легко обратима, то взяв случайные $x_1 \dots x_{M_{\tilde{f}}-1}, x_{M_{\tilde{f}}+1} \dots x_n$, вычислив результаты $M_1(x_1) \dots M_{M_{\tilde{f}}-1}(x_{M_{\tilde{f}}-1}) \dots M_{M_{\tilde{f}}+1}(x_{M_{\tilde{f}}+1}) \dots M_n(x_n)$ и дописав их к $\tilde{f}(x)$, обратим полученное значение и выделим оттуда $x_{\tilde{f}}$, получим обратимость для $\tilde{f}$, но она

односторонняя, удовлетворяет, значит,
Эл ~~[illegible]~~ой – односторонняя универсальная.

Конева

№2

а) Пусть $\xi(x)$ – сильноодносторонняя

$f(x) = \xi(x)$

$$g(x) = \begin{cases} \xi(x), & x \neq 0^n, x \neq 1^n \\ \widetilde{\xi(1^n)}, & x = 1^n \\ \widetilde{\xi(0^n)}, & x = 0^n \end{cases}$$

Тогда $g(x) = \xi(x)$ везде, кроме 2 значений, значит, $f(x)$ и $g(x)$ – сильноодносторонние, и $f \neq g$

$$h(x)|_i = \begin{cases} \xi(x)|_i, & i \not\vdots 2 \\ \xi(x)|_i, & i \vdots 2 \end{cases} \text{ при } x \neq 0^n, x \neq 1^n.$$

Тогда $h(x) = \xi(x)$ везде, кроме 2 значений, значит $h(x)$ – сильноодносторонняя.

б) $$f(xy)|_i = \begin{cases} y|_{\frac{i}{2}}, & i \not\vdots 2 \\ \xi_1(x)|_{\frac{i}{2}}, & i \vdots 2. \end{cases} \qquad g(xy)|_i = \begin{cases} x|_{\frac{i}{2}}, & i \vdots 2 \\ \xi_2(y)|_{\frac{i}{2}}, & i \not\vdots 2 \end{cases}$$

Пусть $\xi_1(x): \{0,1\}^{[\frac{n}{2}]} \to \{0,1\}^{[\frac{n}{2}]}$, $\quad \xi_2(y): \{0,1\}^{[\frac{n+1}{2}]} \to \{0,1\}^{[\frac{n+1}{2}]}$

x длины $[\frac{n}{2}]$, y длины $[\frac{n+1}{2}]$

Тогда $$h(xy)|_i = \begin{cases} y|_{\frac{i}{2}}, & i \not\vdots 2 \\ x|_{\frac{i}{2}}, & i \vdots 2 \end{cases}$$, то есть внутри $h(xy)$ содержатся сами x и y, значит, $h(xy)$ – даже не слабо односторонняя.

Допустим, $f(xy)$ – не сильноодносторонняя, тогда

$$\exists p \; \exists R \; \forall N \; \exists n \geq N : \; P_{xy}\{f(R(f(xy))) = f(xy)\} \geq \frac{1}{p(n)}$$

то есть правильно обратим хотя бы $\frac{2^n}{p(n)}$ значений

различных y – $2^{\left[\frac{n+1}{2}\right]}$, тогда есть такой y_0, что

среди всех значений $x y_0$ обратим правильно

хотя бы $\frac{2^{\left[\frac{n}{2}\right]}}{p(n)}$, то есть $P_x(f(R(f(xy_0)))=f(xy_0))\geq$

$\geq \frac{1}{p(n)}$.

$P_x(\xi(R'(\xi(x)))=\xi(x))\geq\frac{1}{p(n)} \Rightarrow \xi(x)$ – не сильно односторонняя, противоречие.

$R' = R$, из которого взяли x и в ~~кон~~ алгоритм которого вшили значение y_0

аналогично $g(xy)$ – сильноодносторонняя.

в.) ~~$f(x) = \{ f$ из пункта б~~

~~$f(11x) = 11 f_б(x)$ – f из пункта б (из половины там и на $k-1$)~~

~~$f(00x) = 11 f_a(x)$, f из пункта а~~

$$f(x)=\begin{cases} f_б(x), & \text{если } x = 0x_1\\ f_a(x), & \text{если } x = 1x_1\end{cases}, \quad x_1 \text{ длины } k-1$$

$f_a, f_б$ – f из пунктов а и б соответственно.

аналогично $$g(x)=\begin{cases} g_б(x), & \text{если } x = 0x_1\\ g_a(x), & \text{если } x = 1x_1.\end{cases}$$

Тогда если $x=0x_1$, то $h=h_б$, значит, h легко обратима хотя бы на половине x, значит, h – не сильно односторонняя;
если $x=1x_1$, то $h=h_a$, и значит на половине x
h сложно обратить, значит, h – слабо односторонняя.
f и g – сильноодносторонние, т.к. $g_a, g_б$ и $f_a, f_б$ – сильноодносторонние.

№3

а) Пусть g — односторонняя, и $g(0^n) \neq 0^n$. Тогда определим $f(x) = \begin{cases} g(x), & x \neq 0^n \\ 0^n, & x = 0^n \end{cases}$. Так как изменили значение только на 1 аргументе из 2^n, то для любого обратителя $P_x(f(R(f(x))) = f(x)) \leq P_x(g(R(g(x))) = g(x)) + \frac{1}{2^n} < \frac{1}{p(|x|)}$, где p — полином, если g была сильно односторонней, и $<$ $1 - \frac{1}{p(|x|)}$, если слабо односторонней.

Значит, f — односторонняя.

б) если $g(x) = x$ для доли ~~…~~ меньше чем $a(|x|)$, то аналогично пункту а) сделаем не более $a(|x|) \cdot 2^n$ замен, тогда

$P_x(\ldots) \leq \frac{1}{p(|x|)} + a(|x|) < \frac{1}{p_1(|x|)}$ (т. к. это верно $\forall p$ - полинома и $a(|x|) \to 0$ быстрее обратного полинома)

для сильноодносторонней, аналогично для слабоодносторонней

если $g(x) = x$ для доли ~~$\beta(|x|) > a(|x|)$~~ $\beta(|x|) > a(|x|)$, то: если $\exists\, p(|x|)$: $\frac{1}{p(|x|)} < \beta(|x|)$, то для обратителя $R = id$ будет $P_x(g(R(g(x))) = g(x)) \geq \frac{\beta(|x|) \cdot 2^n}{2^n} > \frac{1}{p(|x|)}$, значит, g — не сильно односторонняя.

если $\forall p(|x|)$ ~~$\beta(|x|) <$~~ $a(|x|) < \beta(|x|) < \frac{1}{p(|x|)}$, то сделаем замену на доле $\beta(|x|) - a(|x|)$, где $g(x) = x$ на $\neg x$.

Тогда ~~по первой~~ количество легко обращаемых увеличится не значительно больше, чем на $\beta(|x|)-\alpha(|x|)$, и функция останется односторонней

№ 4

g_i не обязательно будет перестановкой, и это не зависит от i:

если $h(x)$ принимает 0 на 2^{n-1} значениях и 1 на 2^{n-1} значениях, то $h_1(x) = \begin{cases} h(x), & x \neq 0^n \\ \neg h(x), & x = 0^n \end{cases}$ принимает 0 или 1 на $2^{n-1}-1$ значениях, и всё ещё является трудным битом, так как значение изменено на $\frac{1}{2^n}$ доле. Тогда $g_i'(x)$ не является перестановкой, т.к. на ~~каждой~~ i-той позиции 0 и 1 принимаются разное количество раз, где g_i' — это g_i с заменой h на h_1.

если $h(x)$ принимает 0 или 1 на $\leq 2^{n-1}-1$ значениях, то $g_i(x)$ — не является перестановкой.

№7. $X_n \sim U\{0,1\}^{|G(s)|}$.

$G'(s) = 0^{|G(s)|}$, если s сод. ровно $\frac{|s|}{2}$ единиц, и $G'(s) = G(s)$ иначе.

~~Pr(An(Xn)~~ Пусть $|s| = n$, $|G(s)| = k$

$$|Pr(An(X_n)=1) - Pr(An(G'(s))=1)| \geq ||Pr(An(X)=1) - Pr(An(G(s))=1)| -$$

$$- |Pr(An(G(s))=1) - Pr(An(G'(s))=1)| \geq$$

$$\geq |Pr(An(G(s)=1)) - Pr(An(G'(s))=1)| - \frac{1}{p(n)} \quad \forall p \text{ - полинома}$$

$|Pr(An(G(s))=1) - Pr(An(G'(s))=1)| =$ ~~PP(Bs ровно~~

$B - \{s : B\ s$ ровно $\frac{n}{2}$ единиц$\}$

$C - \{s : B\ s$ ровно не $\frac{n}{2}$ единиц$\}$

$$= |Pr(B) \cdot (Pr(An(G(s))=1|B) - Pr(An(G'(s))=1|B) +$$

$$+ Pr(C) \cdot (Pr(An(G(s))=1|C) - Pr(An(G'(s))=1|C)| =$$

$$= |Pr(B) \cdot (Pr(An(G(s))=1|B) - Pr(An(0^k)=1|B)) +$$

$$+ Pr(C) \cdot \underbrace{(Pr(An(G(s))=1|C) - Pr(An(G(s))=1|C)}_{0}| =$$

$$= Pr(B) \cdot |Pr(An(G(s))=1|B) - Pr(An(0^k)=1|B)| \quad =$$

$$Pr(B) = \frac{C_n^{\frac{n}{2}}}{2^n} \sim \frac{\frac{2^n}{\sqrt{\frac{\pi}{2}n}}}{2^n} = \frac{1}{\sqrt{\frac{\pi}{2}n}} \text{ - обратный полином}$$

Возьмем A_n: ~~$An(0^k) = 1$, иначе $An($~~

$An(X) = 1$, если $X = 0^k$, иначе $An(X) = 0$.

Тогда $Pr(An(X_n)=1) = \frac{1}{2^n}$, значит, и $Pr(An(G(s))=1) < \frac{1}{p(n)}$ $\forall p$ - полинома

$$= \frac{C_n^{\frac{n}{2}}}{2^n} \cdot (1 - \alpha(n)),$$ где $\alpha(n) < \frac{1}{p(n)}$ $\forall p$ — полинома

$$\geq \frac{C_n^{\frac{n}{2}}}{2^n} \cdot \frac{1}{2}$$, значит,

для такого A_n X_n и $G'(s)$ вычислительно отличимы

Значит, $G'(s)$ — не ГПСЧ.

$G''(s) = 0^k$, если в s ровно $\frac{n}{3}$ единиц, и $G''(s) = G(s)$ иначе.

$$|Pr(A_n(X_n)=1) - Pr(A_n(G''(s))=1)| \leq$$

$$\leq |Pr(A_n(X_n)=1) - Pr(A_n(G(s))=1)| + |Pr(A_n(G(s))=1) - Pr(A_n(G''(s))=1)| \leq$$

$$\leq \frac{1}{p(n)} + |Pr(B)(Pr(A_n(G(s))=1|B) - Pr(A_n(G''(s))=1|B)) +$$

$\forall p$ — полинома

$B = \{s : $ в s ровно $\frac{n}{3}$ единиц$\}$

$C = \{s : $ в s ровно не $\frac{n}{3}$ единиц$\}$

$$+ Pr(C) \cdot Pr(A_n(G(s))=1|C) - Pr(A_n(G''(s))=1|C)| \leq$$

$$\leq \frac{1}{p(n)} + Pr(B) \cdot (1+1) + Pr(C) \cdot |Pr(A_n(G(s))=1|C) -$$

$$- Pr(A_n(G(s))=1|C)| = \frac{1}{p(n)} + 2Pr(B) < \cancel{\leq \frac{1}{p(n)} + \frac{2}{q(n)} \leq \frac{1}{s(n)}}$$

$\cancel{\forall q}$

$$Pr(B) = \frac{C_n^{\frac{n}{3}}}{2^n} \sim \frac{1}{\sqrt{2\pi \cdot \frac{1}{3} \cdot \frac{2}{3} n}} \cdot 3^{\frac{n}{3}} \cdot \left(\frac{3}{2}\right)^{\frac{2}{3}n} / 2^n =$$

$$= \frac{3^n}{\sqrt{\frac{4\pi}{9} n} \cdot 2^{\frac{5n}{3}}} = \frac{3}{2\sqrt{\pi n}} \cdot e^{n\left(\frac{\ln 27 - \ln 32}{3}\right)} =$$

$$= \frac{3}{2\sqrt{\pi n}} \cdot \left(\frac{27}{32}\right)^{\frac{n}{3}}$$ ~~обратный полином на экспоненту~~

$\frac{27}{32} < 1$, значит, $Pr(B) < \frac{1}{q(n)}$ $\forall q$ – полином

~~значит,~~

$< \frac{1}{p(n)} + \frac{2}{q(n)}$ $\forall p, q$ – полином, значит,

$|Pr(A_n(X_n)=1) - Pr(A_n(G''(S))=1)| < \frac{1}{p(n)}$ $\forall p$ – полином,

значит, G'' – ГПСЧ

№5.

б) $\Rightarrow$ а)

б) $\tilde{f}(x,y) = \begin{cases} (g(x,y), \cancel{\ldots} 0^{n-1}), & \text{если } x \in A \\ f(x,y), & \text{если } x \notin A. \end{cases}$

где $g(x,y)$ – предикат, $f(x,y)$ – сильно одностороняя функц., $P_x(A) = \frac{3}{4}$

для $\tilde{f}(x,y)$ $g(x,y)$ – не трудный, т.к. есть обратн. C:

(например A – все x и y такие, что x и y начинаются с 0)

$C(\tilde{f}(x,y)) = \tilde{f}(x,y)|_1 = \begin{cases} g(x,y), & \text{если } x \in A \\ f(x,y)|_1, & \text{если } x \notin A \end{cases}$

$P_x(C(\tilde{f}(x,y)) = g(x,y)) \geq \frac{3}{4}$

допустим, g – не одностороняя.

$Pr_x(g(R(g(x,y))) = g(x,y)) \geq 1 - \frac{1}{p(n)}$

$Pr_x(g(R(g(x,y))) = g(x,y) \mid X \setminus A) \cdot P(X \setminus A) + Pr_x(g(R(g(x,y))) = g(x,y) \mid A) \cdot Pr(A) \geq 1 - \frac{1}{p(n)}$

$Pr(A) = \frac{3}{4}$, $Pr_x(g(R(g(x,y))) = g(x,y) \mid A) \leq 1$

~~$Pr_{X/A}(g(R(f(x,y))) = f(x,y)) \cdot \frac{1}{4} \geq \frac{1}{4} - \frac{1}{p(n)}$~~

тогда с вероятностью хотя бы $\frac{1}{4} - \frac{1}{p(n)}$ $\forall p$ - полином

умеем обращать $f(x,y)$, но она сильнооднонаправленная,

противоречие.

№8. поставим, на месте конкатенации x и y;

Пусть $G(x,y)$ - ГПСЧ. $|x| = |y| = n$

$$G_1(x,y) = \begin{cases} G(x,y), \text{ если } x \neq y & \text{- таких } 2^{2n} - 2^n \\ 0^{|G(x,y)|}, \text{ если } x = y. & \text{- таких } 2^n \end{cases}$$

$|G(x,y)| = k$

$|Pr_{x,y}(An(X_n) = 1) - Pr_{x,y}(An(G_1(x,y)) = 1)| \leq$

$\leq |Pr_{x,y}(An(X_n) = 1) - Pr_{x,y}(An(G(x,y)) = 1)| +$

$+ |Pr_{x,y}(An(G(x,y)) = 1 | x = y) - Pr_{x,y}(An(G_1(x,y)) = 1 | x = y)| \times$

$\times Pr_{x,y}(x = y) + |Pr_{x,y}(An(G(x,y)) = 1 | x \neq y) - Pr_{x,y}(An(G_1(x,y)) = 1 |$

$x \neq y)| \cdot Pr(x \neq y) < \frac{1}{p(n)} + 2 \cdot \frac{1}{2^n} + \underbrace{|Pr_{x,y}(An(G(x,y)) = 1 | x \neq y) -}$

$\forall p$ - полином

$\underbrace{- Pr_{x,y}(An(G(x,y)) = 1 | x \neq y)|}_{=0} \cdot 1 = \frac{1}{p(n)} + \frac{1}{2^{n-1}} < \frac{1}{q(n)}$ $\forall q$ - полином

Значит, $G_1(x,y)$ - ГПСЧ

$G_1'(x) = G_1(x,x) = 0^k$ - не ГПСЧ, но G_1 - ГПСЧ