Задача 1

P входит в NP т.к. если существует алгоритм, выполняющийся за полиномиальное время на детерминированной МТ, то этот же алгоритм можно выполнить на недетерминированной МТ за то же время (просто все переходы будут детерминированными).

P входит в RP т.к. если существует алгоритм, выполняющийся за полиномиальное время на детерминированной МТ, то этот же алгоритм можно выполнить на вероятностной МТ, задав каждому правилу перехода детерминированного алгоритма вероятность 1. При этом алгоритм выдаст правильный ответ с вероятностью 1, время работы будет таким же (т.е. условия принадлежности к классу RP будут выполнены).

RP входит в NP, т.к. алгоритм для вероятностной МТ можно легко превратить в алгоритм для недетерминированной МТ, заменив вероятностные переходы на недетерминированные (т.е. вместо выбора одного перехода с некоторой вероятностью, МТ будет выполнять сразу все возможные переходы), время работы останется тем же.

RP входит в BPP, т.к. BPP накладывает более слабые ограничения на вероятность ошибки (в остальном (время, вид МТ) условия принадлежности к классам одинаковые).

NP входит в PSPACE т.к.

1. NP входит в NPSPACE т.к. за один шаг МТ может заполнить только одну ячейку памяти, т.е. память не больше времени
2. NPSPACE=PSPACE, т.к. на детерминированной МТ можно сэмулировать недетерминированную, выполняя нечто вроде поиска в ширину по состояниям (т.е., вместо всех недетерминированных переходов сразу, сохранять текущее состояние, выполнять один переход и т.д., а в случае неудачи - возвращаться и пытаться выполнить следующий из возможных переходов). При этом, максимальная глубина рекурсии при поиске в ширину будет полиномиальной, значит общее использование памяти - тоже полиномиальным. Формальное доказательство - теорема Сэвича.

Является ли какое-то из этих включений равенством или строгим включением никто не знает.

Задача 2

Рассмотрим МТ, которая ничего не делает, т.е. просто оставляет входные данные как есть в качестве ответа (с вероятностью 1 сразу переходит в конечное состояние). Для входных $x \in B^*$ из равномерного распределения, x будет заканчиваться на 0 с вероятностью 0.5. Т.к. $g(x)$ не изменяет такие x, то $g^{-1}(x0) = x0$, т.е. такая МТ вероятностью 0.5 найдёт обратное значение. Таким образом, функция g не сильно одностороняя, т.к. вероятность найти обратное значение сильно односторонней функции должна быть пренебрежимо мала для любых полиномиальных вероятностных МТ.

Очевидно, функция g полиномиально вычислима (т.к. она легко выражается через f, которая слабо односторонняя, а значит полиномиально вычислима). Также функция g честная, т.к. она, как и f, сохраняет длину. Предположим, что функция g не является слабо односторонней. Тогда для любого полинома $p(n)$ существует ПВМТ A, такая что:

$$\forall n_0 \in \mathbb{N} \;\; \exists n \geq n_0 \mid \Pr_{x \in_U \mathbb{B}^n}[A(g(x)) \in g^{-1}(g(x))] > 1 - \frac{1}{p(n)} \quad (1)$$

Также нам известно, что f слабо одностороняя, т.е.

$$\exists p'(n) \mid \forall A' \;\; \exists n'_0 \in \mathbb{N} \mid \forall n' \geq n'_0 \Pr_{x \in_U \mathbb{B}^{n'}}[A'(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p'(n')} \quad (2)$$

Зафиксируем такой полином $p'(n)$. Воспользуемся тем, что $g(x1) = f(x)1$(значит, $g^{-1}(f(x)1) = f^{-1}(f(x))1$), и в качестве A' выберем такую ВМТ, которая дописывает ко входу справа единицу, возвращается в начальное положение, запускает алгоритм обращения функции g, а конкретно, запускает ту A, которая существует для полинома $p(n) = 2p'(n-1)$ по формуле (1), а после завершения A удаляет единицу справа (очевидно, A' тоже будет полиномиальной, т.к. Aполиномиальна, а дополнительные операции выполняются за линейное время). При этом:

$$\Pr_{x \in_U \mathbb{B}^{n'}}[A'(f(x)) \in f^{-1}(f(x))] = \Pr_{x \in_U \mathbb{B}^{n'}}[A(g(x1)) \in g^{-1}(g(x1))] \quad (3)$$

Для выбранной A' зафиксируем существующее n'_0 из формулы (2):

$$\forall n' \geq n'_0 \;\; \Pr_{x \in_U \mathbb{B}^{n'}}[A'(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p'(n')} \quad (4)$$

Подставим $m = n'_0 + 1$и выбранный ранее полином в (1):

$$\exists n \geq m \mid \Pr_{x \in_U \mathbb{B}^n}[A(g(x)) \in g^{-1}(g(x))] > 1 - \frac{1}{2p'(n-1)} \quad (5)$$

Зафиксируем существующее n из (5) и подставим n - 1 ($n - 1 \geq n'_0$ т.к. $n \geq m$) в (4):

$$\Pr_{x \in_U \mathbb{B}^{n-1}}[A'(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p'(n-1)} \quad (6)$$

Ура, кванторы закончились, осталось понять, как связаны вероятности из (3), (5) и (6), для которых у нас уже есть какие-то неравенства:

$$1 - \frac{1}{2p'(n-1)} < \Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}[A(g(x)) \in g^{-1}(g(x))]$$

$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^{n-1}}[A(g(x1)) \in g^{-1}(g(x1))] = \Pr_{x \in_{\mathcal{U}} \mathbb{B}^{n-1}}[A'(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p'(n-1)}$$

Попробуем оценить вероятность (5), чтобы объединить эти неравенства:

$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}[A(g(x)) \in g^{-1}(g(x))] = \frac{1}{2} \Pr_{x \in_{\mathcal{U}} \mathbb{B}^{n-1}}[A(g(x1)) \in g^{-1}(g(x1))] +$$
$$+ \frac{1}{2} \Pr_{x \in_{\mathcal{U}} \mathbb{B}^{n-1}}[A(g(x0)) \in g^{-1}(g(x0))] \leq \frac{1}{2} \Pr_{x \in_{\mathcal{U}} \mathbb{B}^{n-1}}[A(g(x1)) \in g^{-1}(g(x1))] + \frac{1}{2}$$

(из этой оценки становится понятно, зачем выше нужны были именно такие полином и m)

Отсюда:

$$1 - \frac{1}{2p'(n-1)} < \frac{1}{2}\left(1 - \frac{1}{p'(n-1)}\right) + \frac{1}{2}$$

Что приводит к противоречию:

$$2 - \frac{2}{2p'(n-1)} < 1 - \frac{1}{p'(n-1)} + 1$$
$$2 - \frac{1}{1p'(n-1)} < 2 - \frac{1}{p'(n-1)}$$
$$0 < 0$$

Значит, функция g слабо односторонняя.

Задача 3

Пусть существует некоторая односторонняя функция g(x). Тогда её можно преобразовать в одностороннюю функцию f(x), которая сохраняет длину аргумента. Рассмотрим язык

$L = \{(z, y) \mid z, y \in B^*;\ |z| = k \leq n = |y|;\ \exists x \in B^n \mid f(x) = y;\ substr(x, 0, k) = z\}$

т.е. набор пар, где z - префикс некоторого x, y - значение f(x). Этот язык принадлежит NP, т.к. полное значение x является сертификатом: зная x, можно за полиномиальное время вычислить y = f(x) и проверить, является ли z префиксом x, тем самым за полиномиальное время (на детерминированной МТ) проверить принадлежность пары (z, y) языку L.

Пусть P=NP. Тогда существует некоторый алгоритм A для детерминированной МТ, который за полиномиальное время проверяет принадлежность тройки языку L. Рассмотрим алгоритм, который с помощью A обращает f(x):

1. Принять на вход y

2. Инициализировать z пустой строкой, k = 0 (длина z), n = |y|
3. Если k == n, то вернуть z
4. С помощью A проверить, принадлежит ли пара (z0, y) языку L
5. Если принадлежит, то дописать 0 к z
6. Иначе, дописать 1 к z
7. k = k + 1
8. goto 3

Т.е. на каждом шаге мы с помощью A пытаемся угадать следующий бит x, собирая x по одному биту и проверяя, принадлежит ли пара с таким префиксом языку L.

Этот алгоритм содержит только один цикл, который выполняет ровно n итераций, а на каждой итерации выполняет полиномиальный алгоритм A, т.е. этот алгоритм тоже полиномиальный. И детерминированный. Можно адаптировать его для ПВМТ, задав каждому переходу вероятность 1. Такая ПВМТ с вероятностью 1 найдёт обратное значение f(x), значит функция f(x) не односторонняя, противоречие. Значит, P!=NP.

Задание 4

Пусть f(x) - односторонняя функция. Предположим, что мощность множества значений меньше некоторого полинома, т.е.

$$\exists p(n) \mid \forall n_0 \in \mathbb{N}\ \exists n \geq n_0 \mid \ |\{f(x) \mid x \in \mathbb{B}^n)\}| \leq p(n)$$

Выпишем определение одностороннести для f(x) и выпилим кванторы (как в задании 2), выбрав в качестве A такую ПВМТ, которая генерирует случайное x’ длины n из равномерного распределения. Получим два неравенства:

$$|\{f(x) \mid x \in \mathbb{B}^n)\}| \leq p(n)$$
$$\Pr_{x \in_U \mathbb{B}^n}[A(f(x)) \in f^{-1}(f(x))] < \frac{1}{p(n)}$$

Пусть $k = |\{y \mid y = f(x);\ x \in B^n\}|$, a_1, …, a_k - вероятности того, что для случайного $x \in B^n$ функция вернёт соответствующий $y_i = f(x)$. Очевидно, $\Sigma_{i=1}^{k} a_i = 1$.

Внимательно посмотрим на вероятность того, что A угадает обратное значение:

$$\Pr_{x\in\mathcal{U}\mathbb{B}^n}[A(f(x)) \in f^{-1}(f(x))] = \Pr_{x\in\mathcal{U}\mathbb{B}^n, x'\in\mathcal{U}\mathbb{B}^n}[x' \in f^{-1}(f(x))] =$$

$$= \Pr_{x\in\mathcal{U}\mathbb{B}^n, x'\in\mathcal{U}\mathbb{B}^n}[f(x') = f(x)] = \sum_{i=1}^{k} \Pr_{x\in\mathcal{U}\mathbb{B}^n, x'\in\mathcal{U}\mathbb{B}^n}[f(x') = y_i \wedge f(x) = y_i] =$$

$$= \sum_{i=1}^{k} a_i a_i \geq \frac{1}{k} \geq \frac{1}{p(n)}$$

Но в то же время эта вероятность должна быть меньше 1/p(n), противоречие. Значит, мощность множества больше любого полинома:

$$\forall p(n)\ \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0\ |\{f(x)|x \in \mathbb{B}^n)\}| > p(n)$$