Предикат $DISJ_k(x,y)$ определен на парах k-элементных множеств $x, y \subset \{1,2,\ldots,n\}$. Его значение равно 1, если множества не пересекаются.

Теорема. Вероятностная безошибочная сложность этого предиката имеет порядок $R(DISJ_k) = O(k + \log n)$.

Доказательство. Мы знаем, что $R(f) \le (R^1_\varepsilon(f) + R^1_\varepsilon(\neg f))/(1-\varepsilon)$ для любого $\varepsilon < 1$. Поэтому достаточно доказать неравенства $R^1_\varepsilon(DISJ_k) = O(k+\log n)$ и $R^1_\varepsilon(\neg DISJ_k) = O(k+\log n)$ для некоторого фиксированного $\varepsilon < 1$. Мы докажем это для $\varepsilon = 3/4$. Кроме того, можно вспомнить, что переход от общего источника случайных битов к частному стоит добавления $O(\log\log|X \times Y|)$ переданных битов. В нашем случае X и Y имеют мощность $\binom{n}{k} \le n^k$, следовательно $\log\log|X \times Y| \le 1 + \log k + \log\log n$. Поэтому можно разрешить Алисе и Бобу пользоваться общими случайными битами.

Рассмотрим следующий вспомогательный протокол: Алиса с Бобом интерпретируют общий источник случайных битов как бесконечную последовательность $S_1, S_2, \ldots$ независимых случайных подмножеств множества $\{1,2,\ldots,n\}$ (каждое S_i задается n битами). Сначала Алиса находит первое в последовательности $S_1, S_2, \ldots$ множество S_i, целиком включающее x, и посылает его номер Бобу (такое i найдется с вероятностью 1). Боб, получив i, заменяет y на $y \cap S_i$. Затем Боб находит наименьшее $j > 0$, для которого $y \subset S_{i+j}$ и посылает j Алисе. Алиса, заменяет x на $x \cap S_{i+j}$. Заметим, что выброшенные элементы из x и y не могли принадлежать пересечению $x \cap y$, поэтому в ходе протокола пересечение множеств не изменяется. Будем называть этот обмен одной стадией. Затем тоже самое повторяется еще раз и так бесконечно много раз. На каждой стадии Алиса и Боб используют свежие случайные множества. (Конец вспомогательного протокола.)

Будем говорить, что во вспомогательном протоколе достигнут успех, если для текущих версий x, y выполнено

$$|x| + |y| \le 4|x \cap y|.$$

Если исходные множества не пересекались, то и текущие всегда не пересекаются; в этом случае успех означает, что оба множества x, y стали пустыми и тем самым Алиса с Бобом знают, что исходные множества не пересекались. Если же исходные множества пересекаются, то пересечение текущих множеств всегда не пусто. В этом случае при достижении

успеха $|x \cap y| \geq |x|/2$ или $|x \cap y| \geq |y|/2$. А значит хотя бы один из игроков, при случайном выборе элемента из своего множества, с вероятностью не менее $1/2$ выберет элемент из пересечения $x \cap y$, и послав его другому сможет узнать, что множества пересекаются. Заметим еще, что если в некоторый момент достигнут успех, то и во все будущие моменты выполнено неравенство $|x|+|y| \leq 4|x \cap y|$ (поскольку $x \cap y$ не изменяется, а $|x| + |y|$ может только уменьшаться).

Пусть x и y имеют r общих элементов, а разности $x \setminus y$ и $y \setminus x$ соотвественно p и q элементов. В этих обозначениях условие успеха записывается как $p + q \leq 2r$.

Лемма. Среднее количество переданных битов до достижения успеха во вспомогательном протоколе есть $O(p + q)$.

Доказательство. Сначала поймем, что можно сказать о распределении множества S_i, выбранного Алисой на первой стадии. Оно заведомо включает x, а все элементы вне x принадлежат ему с вероятностью $1/2$, причем включаются в S_i независимо друг от друга. То же самое можно сказать и о множествах, выбранных Алисой на всех остальных стадиях. Поэтому после каждой стадии q в среднем уменьшается вдвое. Аналогичное верно для p.

Теперь оценим среднее количество битов переданных Алисой на одной стадии. На первой стадии оно равно среднему количеству битов в записи i для первого $S_i \supset x$. Для любого фиксированного k вероятность того, что S_k включает x, равна $2^{-|x|}$. Поэтому среднее значение i равно $2^{|x|}$. В силу вогнутости логарфмической функции среднее значение $\log i$ не больше логарифма среднего значения самого i, то есть, не больше $|x|$. То же самое верно для любой стадии. Боб передает в среднем немного меньше битов, поскольку после получения алисиного множества $y \setminus x$ уменьшается в среднем вдвое. Для простоты подсчета мы будем игнорировать это уменьшение, огрубляя тем самым оценку.

Будем доказывать лемму индукцией по $p + q$. Чтобы можно было применить индукцию, нужно, чтобы в ходе каждой стадии $p + q$ уменьшалось. А оно с ненулевой вероятностью может не уменьшиться. Поэтому разделим стадии на два сорта: назовем стадию удачной, если в ходе нее $p+q$ уменьшилось, а остальные стадии будем называть неудачными. Оценим отдельно среднее количество битов переданных на неудачных стадиях.

Пусть в начале стадии $p + q > 2r$. Вероятность того, что стадия неудачна равна 2^{-p-q}. Вероятность того, что к тому же и следующая

стадия будет неудачной равна 2^{-2p-2q}. И так далее. Поэтому среднее количество неудачных стадий до первой удачной равно $2^{-p-q}/(1-2^{-p-q}) \leq 2^{-p-q+1}$. Таким образом, до тех пор, пока $p+q$ не уменьшится, Алиса с Бобом передадут в среднем не более $(p+q+2r)2^{-p-q+1} < (p+q)2^{-p-q+2}$ битов. Отсюда следует, что среднее количество битов, переданных до достижения успеха на всех неудачных стадиях, не превосходит

$$\sum_{2r<i\leq p+q} i2^{-i+2},$$

что ограничено константой, поскольку ряд $i2^{-i}$ сходится.

Теперь оценим по индукции среднее количество битов, переданных до достижения успеха на всех удачных стадиях. Докажем, что оно не больше $4(p+q)$. База индукции: если $p+q=2r$, то успех уже наступил и утверждение очевидно выполнено.

Индуктивный переход. Пусть $p+q > 2r$. Как объяснялось выше, среднее количество битов, переданных в ходе первой удачной стадии, не превосходит $(p+r)+(q+r) < 2(p+q)$. В результате получатся множества x', y', к которым можно применить индуктивное предположение и заключить, что на оставшихся удачных стадиях будет в среднем передано не более $4(p'+q')$ битов. Чему равно среднее значение $p'+q'$? Мы знаем, что в результате выполнения любой стадии среднее значение $p'+q'$ равно $(p+q)/2$. Но у нас есть дополнительное условие об удачном исходе стадии. Среднее значение $p'+q'$ по условному распределению меньше среднего значения по безусловному, поскольку условие в нашу пользу. Поэтому в результате выполнения первой удачной стадии среднее значение $p'+q'$ даже меньше $(p+q)/2$. Итак, среднее значение общего количества переданных битов на всех стадиях до первого успеха не больше $2(p+q)+4((p+q)/2) = 4(p+q)$, что завершает доказательство леммы.

Теперь построим вероятностный протокол вычисления $DISJ_k$ с односторонней ошибкой. По лемме среднее количество битов переданное во вспомогательном протоколе до первого успеха не превосходит $t = O(k)$. Запустим вспомогательный протокол до тех пор, пока множества x, y не станут пустыми или не будет передано $2t$ битов. В первом случае Алиса и Боб останавливаются и выдают положительный ответ (исходные множества не пересекались). Во втором случае они выдают отрицательный ответ. Если исходные множества пересекались, то выданный ответ

правильный с вероятностью 1. Если они пересекаются, то ответ будет неправильным (то есть, отрицательным) только, если после передачи $2t$ битов успех не достигнут. Вероятность этого не превосходит $1/2$.

Построим протокол вероятностный протокол вычисления $\neg DISJ_k$ с односторонней ошибкой. Запустим вспомогательный протокол до тех пор, пока не будет передано $2t$ битов. Если одно из текущих x, y окажутся пустыми, то Алиса и Боб выдают отрицатеьный ответ (множества не пересекаются). Иначе они обмениваются случайными элементами из своих текущих множеств. Если таким образом обнаружится общий элемент, то они выдают положительный ответ. Если исходные множества не пересекаются, то вероятность ошибки равна нулю. Если они пересекаются, то текущие можества всегда пересекаются. С вероятностью не менее $(1/2)(1/2) = 1/4$ Алиса и Боб это обнаружат (первый сомножитель есть вероятность достигнуть успеха, а второй — вероятность найти общий элемент при условии, что успех достигнут). (Конец доказательства.)