Пусть f_n выбирается случайно среди всех биективных функций $f_n : \{0,1\}^n \to \{0,1\}^n$ (все биекции равновероятны). Тогда с вероятностью 1 семейство f_n необратимо. Чтобы убедиться в этом, достаточно доказать, что для любого полиномиального вероятностного алгоритма R для достаточно больших n вероятность того, этот алгоритм R обращает случайно взятое $f_n(x)$ меньше $2^{-n/2}$. Поскольку обращение биективной функции — это то же самое, что вычисление обратной к ней функции, причем обратная функция так же выбирается равновероятно среди всех биекций, достаточно доказать то же самое для задачи вычисления $f_n(x)$. Обозначим через $p_n(f)$ вероятность события "$R(x) = f(x)$" (при случайном выборе x и случайном выборе случайных битов алгоритма R). Среднее значение $p_n(f)$ равно 2^{-n}. (В самом деле, оно равно среднему по всем x и всем случайным битам r алгоритма R доли тех функций f, для которых $f(x)$ равно результату работы R на входе x со случайными битами r; ясно, что эта доля равна 2^{-n}.) Поэтому доля функций f, для которых $p_n(f) > 2^{-n/2}$, меньше $2^{-n/2}$. Поскольку ряд $\Sigma_n 2^{-n/2}$ сходится, по лемме Бореля–Кантелли с вероятностью 1 при случаном выборе f лишь для конечного числа n выполнено неравенство $p_n(f) < 2^{-n/2}$.