טענה 2: $|Good_n| > (1-1/2p(n))\bullet 2^n$

הוכחה:

נניח בדרך השלילה שגודלו של $Good_n$ קטן מ- $(1-1/2p(n))\bullet 2^n$ ונוכיח שאז אלגוריתם B אינו טוב כמובטח. כזכור, מובטח שאלגוריתם B מצליח בהסתברות שנכנה s(n):

$$S(n) = Pr\,[B(g(x)) \in g^{-1}(g(x))] > 1/q(n^2p(n))$$

(כאשר ההסתברות היא על הטלות B ובחירה אחידה של x.)

נפריד את s(n) לשניים לפי השאלה אם $x=x_1x_2\ldots x_{n\bullet p(n)}$ מכיל או לא מכיל תת-מחרוזת x_i שאינה ב-$Good_n$.

$$S(n) = Pr\,[B(g(x)) \in g^{-1}(g(x)) \wedge \exists i\ x_i \notin Good_n] + Pr\,[B(g(x)) \in g^{-1}(g(x)) \wedge \forall i\ x_i \in Good_n]$$

נחסום כל חלק לחוד.

חלק ראשון (הסיכוי להצליח כשיש קלט בעייתי ל-f):

$$Pr\,[B(g(x)) \in g^{-1}(g(x)) \wedge \exists i\ x_i \notin Good_n] \le \qquad (1)$$

$$\sum_{i=1}^{n\bullet p(n)} Pr\,[B(g(x)) \in g^{-1}(g(x)) \wedge x_i \notin Good_n] \le \qquad (2)$$

$$\sum Pr\,[B(g(x)) \in g^{-1}(g(x)) \mid x_i \notin Good_n] \le \qquad (3)$$

$$\sum Pr\,[C(f(x_i)) \in f^{-1}(f(x)) \mid x_i \notin Good_n] \le$$

$$n\bullet p(n) \bullet (n/a(n)) = (n^2p(n)) / (\,2n^2\bullet p(n)\bullet q(n^2p(n))\,) = 1/(\,2q(n^2p(n))\,)$$

הצדקות:

(1) לכל אוסף מאורעות $T1,T2,\ldots,Tk$ מתקיים: $Pr\,[\exists i\ T_i] = Pr[\cup_i T_i] \le \sum_i Pr[T_i]$.

(2) לכל זוג מאורעות $T1$, $T2$ מתקיים: $Pr[T1 \wedge T2] \le Pr[T1 \mid T2]$.

(3) אם B מצליח להפוך את $g(x_1x_2\ldots x_{n\bullet p(n)})$ אז בודאי C מצליחה בהפיכת $f(x_i)$.

חלק שני (הסיכוי גם להצליח וגם שאין קלט בעייתי ל-f):

$$Pr\,[B(g(x)) \in g^{-1}(g(x)) \wedge \forall i\ x_i \in Good_n] \le Pr\,[\forall i\ x_i \in Good_n] \le (1-1/2p(n))^{n\bullet p(n)} < 2^{-n/2}$$

הצדקה: לפי הנחת השלילה $|Goodn| \le (1-1/2p(n))\bullet 2^n$.

סכום שני החלקים:

$$s(n) < 1/(2q(n^2p(n))\,) + 2^{-n/2} < 1/q(n^2p(n))$$

אבל מובטח שאלגוריתם B מצליח בהסתברות:

$$s(n) > 1/q(n^2p(n))$$

ומכאן סתירה.

מ.ש.ל. טענה 2.