## 4.5 The Prediction Test

The extrapolation test looks somewhat strange since it extrapolates the bit sequence in reverse direction, a clear contrast with the usual cryptanalytic procedures that try to predict *forthcoming* bits. We'll immediately remedy this quaint effect:

Let $C = (C_n)_{n\in\mathbb{N}}$ be a polynomial family of circuits,

$$C_n : \mathbb{F}_2^n \times \mathbb{F}_2^{i_n} \times \Omega_n \longrightarrow \mathbb{F}_2$$

with $0 \le i_n \le r(n)-1$, and let $h \in \mathbb{N}[X]$ be a non-constant polynomial. Then $C$ has a $\frac{1}{h}$-advantage for predicting $G$ if the subset of parameters $m \in M$ with

$$P\{(x,\omega) \mid C_n(m, b_1^{(m)}(x), \ldots, b_{i_n}^{(m)}(x), \omega) = b_{i_n+1}^{(m)}(x)\} \ge \frac{1}{2} + \frac{1}{h(n)}$$

is not sparse in $M$. The pseudorandom generator $G$ passes the **prediction test** if no polynomial family of circuits has an advantage for predicting $G$. The proof of "(i) $\Longrightarrow$ (ii)" in Theorem 4 directly adapts to this situation yielding:

**Corollary 1** *Every perfect pseudorandom generator passes the prediction test.*

**Corollary 2** *If the quadratic residuosity conjecture is true, then the BBS generator is perfect, in particular passes the prediction test.*

*Proof.* Otherwise from Proposition 13 we could construct a polynomial family of circuits that decides quadratic residuosity for a non-sparse subset of BLUM integers. ◇

The paper

> U. V. VAZIRANI, V. V. VAZIRANI: Efficient and secure pseudo-random number generation, CRYPTO 84, 193–202

contains a stronger result: *If the factoring conjecture is true, i. e. if factoring large integers is hard, then the BBS generator is perfect.*