A Noise-Adaptive Algorithm for First-Order Reed-Muller Decoding

Jon Feldman
jonfeld@mit.edu

Matteo Frigo
athena@vanu.com

Ibrahim Abou-Faycal
iaboufay@mit.edu

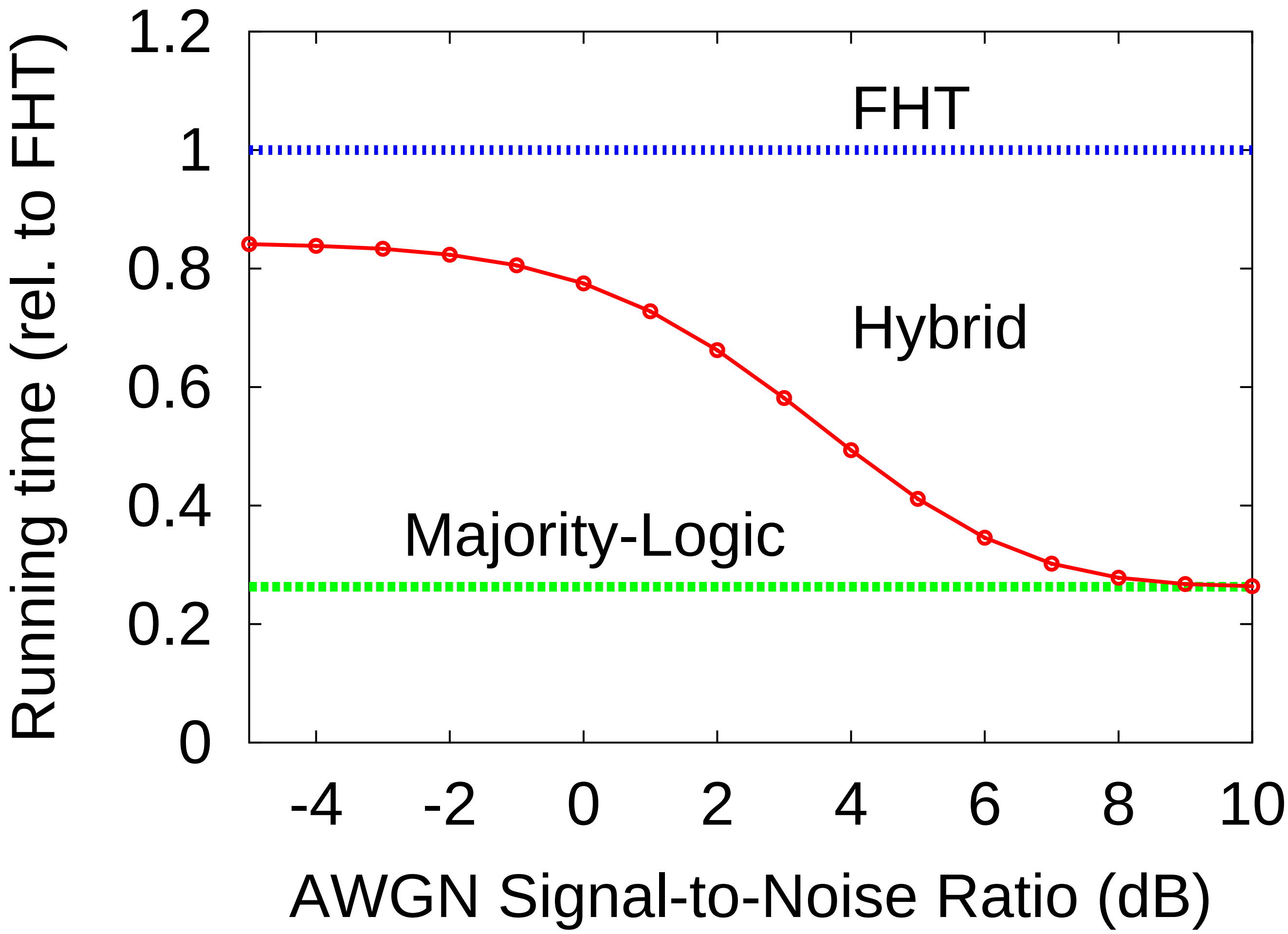
M.I.T.

Vanu, Inc.

CCK demodulation

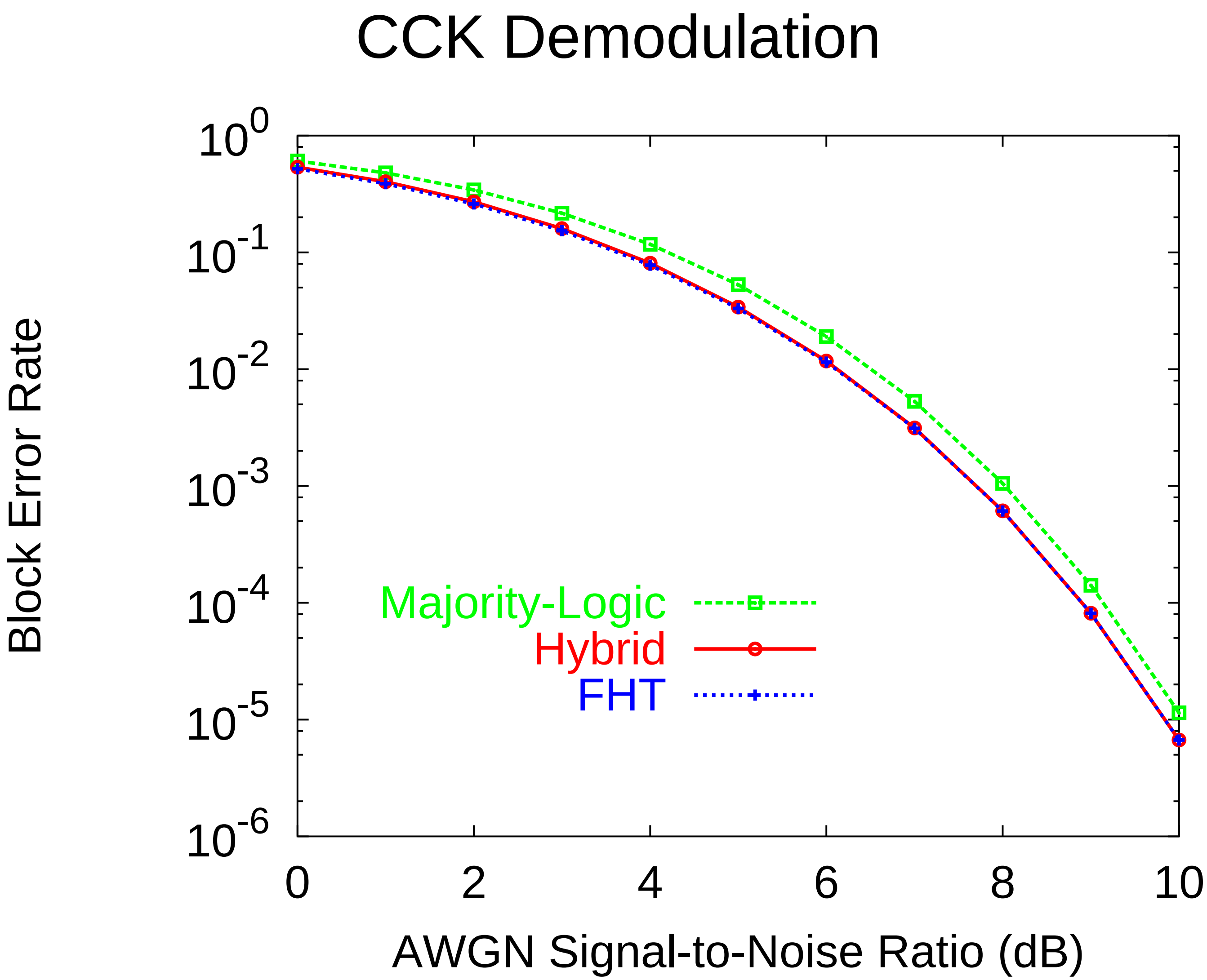
- Demodulation: bottleneck in software 802.11b implementation.
- Standard optimal demodulator based on Fast Walsh-Hadamard transform (FHT);
  - Software radios cannot take advantage of parallelism.
- Majority-logic demodulators [Reed ’54, Massey ’63] efficient but suboptimal.
- Our *Hybrid* algorithm:
  - almost as fast as majority-logic;
  - “almost as optimal” as FHT.

Running Time Comparison



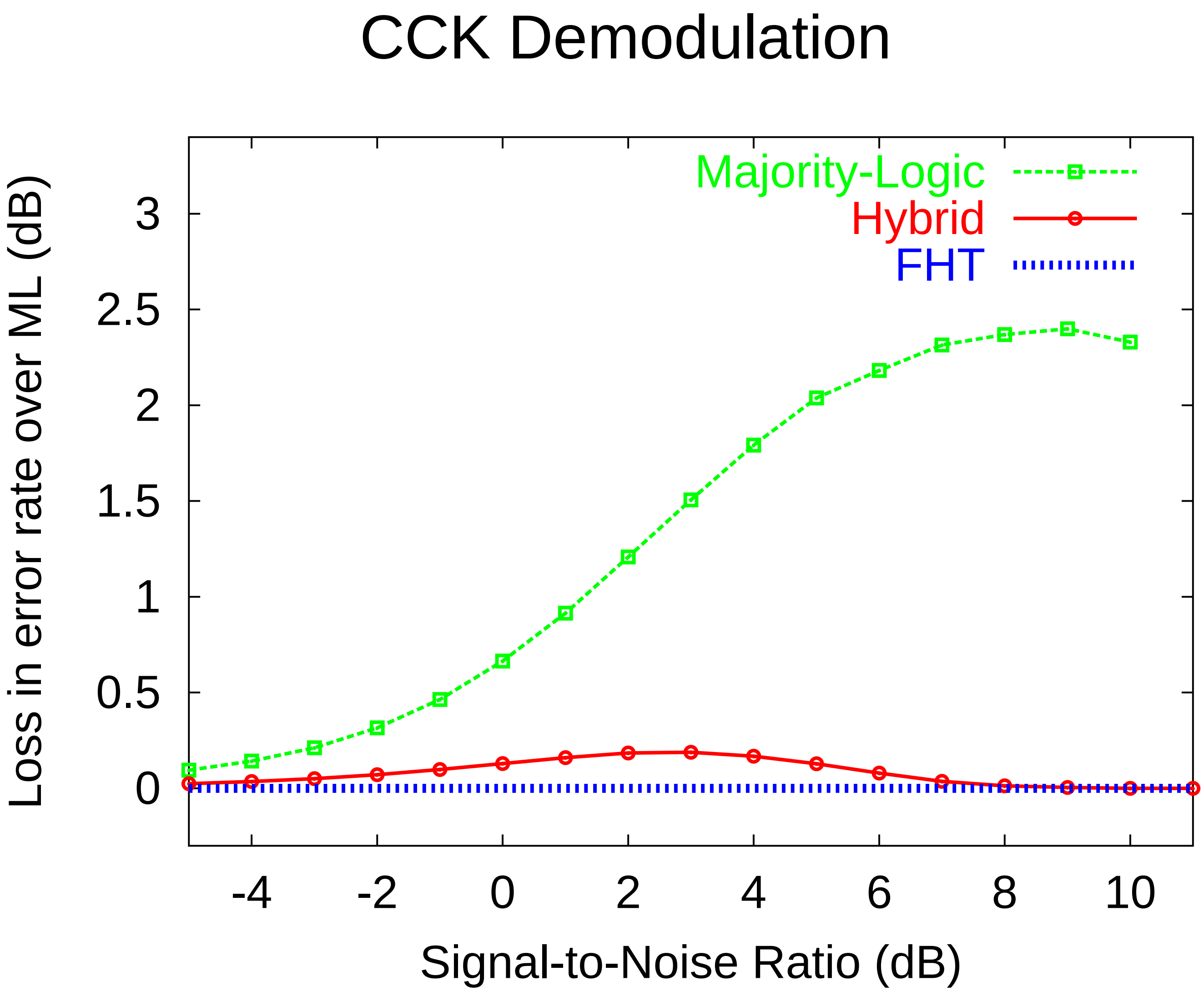
- Running time (implicitly) SNR-dependent
  - OK for software radios.

Performance Comparison



- Hybrid algorithm very close to optimal FHT.

Performance Comparison (closer look)



- Negligible loss of performance ($\leq$ 0.2 dB).

Outline

- CCK modulation / demodulation.
- Majority logic decoding.
- The hybrid algorithm.
- Generalization to first-order Reed-Muller (FORM) codes:
  - H_e: Error rate of Hybrid algorithm.
  - O_e: Error rate of ML decoder (FHT).

$$H_e \leq O_e + exp(-\Omega(n)).$$

CCK modulation

- **Info:** 4 "complex bits:"

$$\phi = (\phi_0, \phi_1, \phi_2, \phi_3) \quad (\phi_i \in Q, \;\; Q = \{1, i, -1, -i\})$$

- **Transmit:** $x(\phi) = (x_0, \ldots, x_7)$, where*:

$$\begin{aligned} x_0 &= \phi_3 & x_4 &= \phi_3 \; \phi_2 \\ x_1 &= \phi_3 \;\;\;\;\;\;\;\; \phi_0 & x_5 &= \phi_3 \; \phi_2 \;\;\;\;\;\; \phi_0 \\ x_2 &= \phi_3 \;\; \phi_1 & x_6 &= \phi_3 \; \phi_2 \; \phi_1 \\ x_3 &= \phi_3 \;\; \phi_1 \; \phi_0 & x_7 &= \phi_3 \; \phi_2 \; \phi_1 \; \phi_0 \end{aligned}$$

- **Receive:** $(y_0, \ldots, y_7)$, $y_i = x_i + N_i(0, \sigma^2)$
- (* In real system, x_1 and x_4 negated.)

CCK demodulators

- Maximum-Likelihood decoding: find $\phi^{\max}$ where

$$\phi^{\max} = \max_{\phi \in Q^4} |x(\phi) \cdot y|, \qquad (Q = \{1, i, -1, -i\}).$$

  - Can be computed via Fast Hadamard Transform (FHT).
  - FHT not fast enough for software radio.

- Majority-Logic [Reed '54, Massey '63] decoding:
  - Extract "votes" for each information symbol.
  - Tally votes, majority rules for each symbol.
  - Use for CCK: [van Nee '96, Paterson/Jones '98].

Majority-Logic Decoding for CCK

$$
\begin{array}{lllllllllll}
x_0 & = & \phi_3 & & & \qquad & x_4 & = & \phi_3 & \phi_2 & & \\
x_1 & = & \phi_3 & & \phi_0 & \qquad & x_5 & = & \phi_3 & \phi_2 & & \phi_0 \\
x_2 & = & \phi_3 & \phi_1 & & \qquad & x_6 & = & \phi_3 & \phi_2 & \phi_1 & \\
x_3 & = & \phi_3 & \phi_1 & \phi_0 & \qquad & x_7 & = & \phi_3 & \phi_2 & \phi_1 & \phi_0
\end{array}
$$

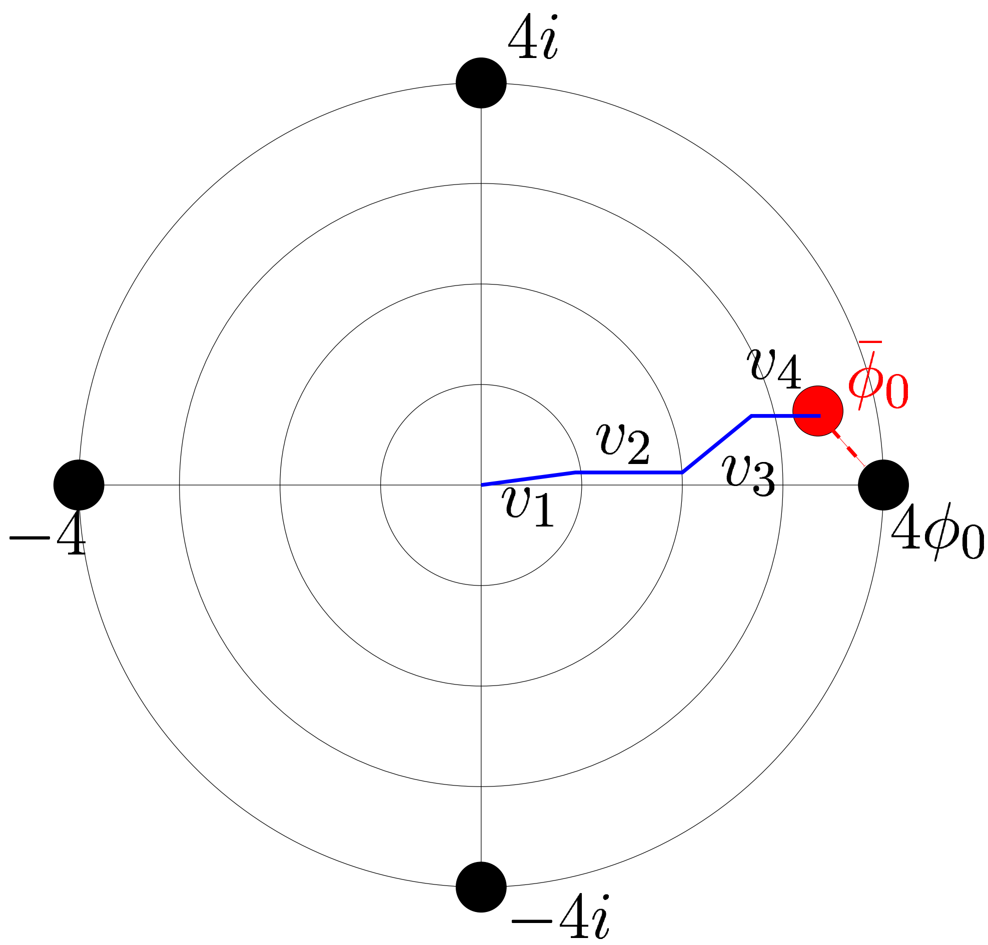
- Example: $x_3 x_2^* = (\phi_3 \phi_1 \phi_0)(\phi_3 \phi_1)^* = \phi_3 \phi_1 \phi_0 \phi_3^* \phi_1^* = \phi_0$

- This makes $y_3 y_2^*$ a "vote" for ϕ_0:

$$
\begin{aligned}
E\left[y_3 y_2^*\right] &= E\left[(x_3 + N_3)(x_2 + N_2)^*\right] \\
&= E\left[(x_3 + N_3)\right] E\left[(x_2^* + N_2^*)\right] \\
&= x_3 x_2^* \\
&= \phi_0
\end{aligned}
$$

- Four independent votes for ϕ_0: $y_1 y_0^*$, $y_3 y_2^*$, $y_5 y_4^*$, $y_7 y_6^*$

Tallying "Soft" Votes



- Suppose $\phi_0 = 1$.
- Four votes:

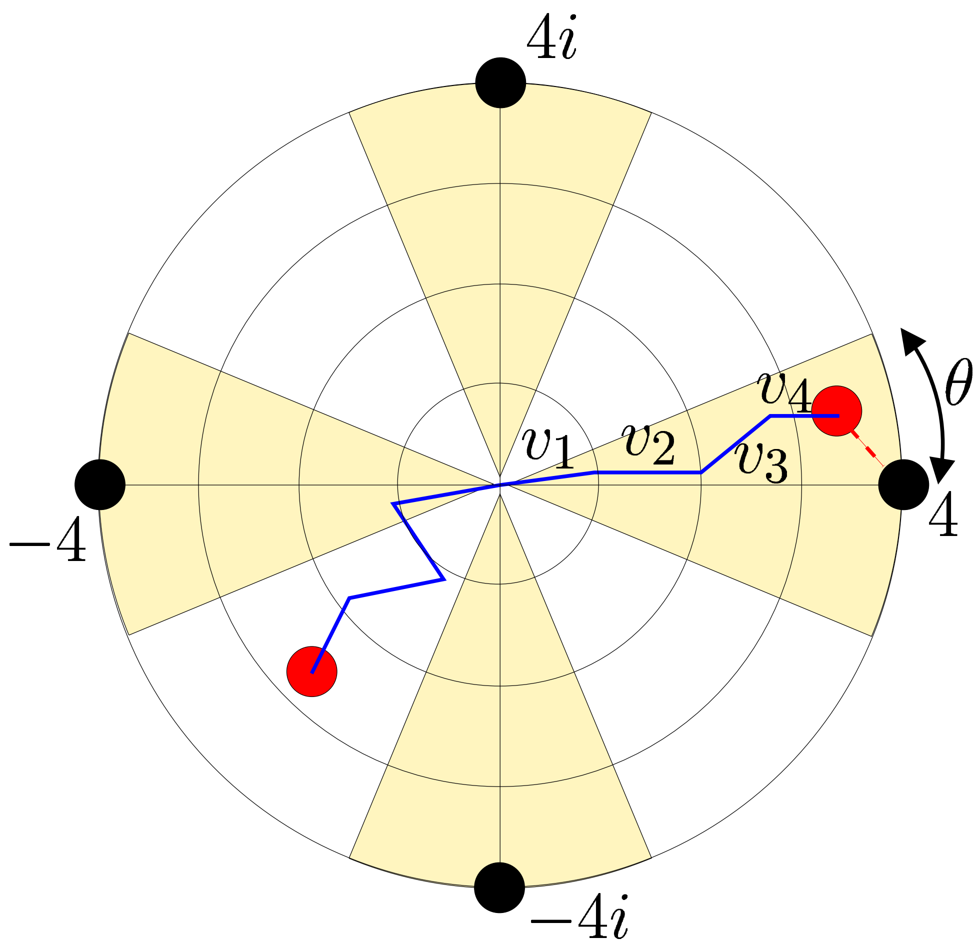
  $v_1 = y_1 y_0^*$ $\quad v_2 = y_3 y_2^*$

  $v_3 = y_5 y_4^*$ $\quad v_4 = y_7 y_6^*$.
- "Estimate" $\bar{\phi}_0$:

$$\bar{\phi}_0 = \sum_{i=1}^{4} v_i \approx 4\phi_0 = 4$$

- Set ϕ_0 to "closest" point in $\{4, 4i, -4, -4i\}$.

The Hybrid Algorithm



- Set "threshold angle" θ.
  - $\theta = \tan^{-1}(2/3)$
- Compute est. $\bar{\phi}_0$, $\bar{\phi}_1$, $\bar{\phi}_2$.
- Find closest $\phi_i \in Q$ for each estimate:

$$\phi_i = \arg\min_{\phi \in Q} |\angle(\phi) - \angle(\bar{\phi}_i)|.$$

- If $|\angle(\bar{\phi}_i) - \angle(\phi_i)| > \theta$ for *any* $i \in \{0, 1, 2\}$, run FHT.
- Otherwise, compute ϕ_3 from ϕ_0, ϕ_1, ϕ_2.

General FORM Codes

- Definition of $FORM_q(k,p)$:
  - Information word $c \in \mathbb{Z}_q^k$.
  - Polynomial $P(x) = c^T x$, where $x \in \{0, \ldots, p-1\}^k$ for some $p \leq q$.
  - Codeword: Evaluate $P(x) \bmod q$ for all possible values of x. Code length $n = p^k$.
- Classic Reed-Muller codes: $p = 2$.
- Hadamard Codes: $FORM_2(k,2)$.
- CCK: isomorphic to $FORM_4(3,2)$.
- Generalized version of hybrid algorithm works for any FORM code.

Coding Theorem for AWGN Channel

- H_e: Error rate of Hybrid algorithm.
- O_e: Error rate of ML decoder (FHT).
- Theorem: For all $0 < \alpha < 1$, $0 < t < 1$,

$$H_e \leq O_e + exp\left(-A_1 n\right) + exp\left(-A_2 n\right).$$

$$\begin{aligned} A_1 &= \frac{(1-\alpha)^2 \sin^2(2\pi/q - \theta)}{8\sigma^2} \\ A_2 &= \frac{1}{2}\left(\frac{t\alpha \sin(2\pi/q - \theta)}{\sigma^2} - \ln\left(\frac{t \arccos(-t)}{(1-t^2)^{3/2}} + \frac{1}{1-t^2}\right)\right) \end{aligned}$$

- Example: $q = 4$ (QPSK), $\theta = \tan^{-1}(2/3)$, SNR > 4 dB,

$$H_e \leq O_e + 2^{1-n/10}.$$

Conclusion

- Hybrid algorithm for CCK:
  - Provides “near-optimal” decoding,
  - Runs at a fraction of the running time,
  - Allows software implementation of 802.11b.
- For any FORM code:

$$H_e \leq O_e + exp(-\Omega(n)).$$