tapered active region and buried facets, polarisation-insensitive operation within 0·5 dB is obtained. Further, we have investigated the influence of AM-crosstalk-induced power penalties on the number of WDM channels. For a 1 dB penalty ~12 channels can be transmitted simultaneously.

Acknowledgments: Part of this work was supported by France Telecom and RACE project 1027.

28th August 1992

L. Eskildsen, B. Mikkelsen, T. Durhuus, C. G. Joergensen and K. E. Stubkjaer (*Center for Broadband Telecommunications, Electromagnetics Institute, Technical University of Denmark, Building 348, DK-2800 Lyngby, Denmark*)

P. Doussière, P. Garabédian, F. Leblond, J.-L. Lafragette and B. Fernier (*Alcatel Alsthom Recherche, F-91460 Marcoussis, France*)

References

1 MERSALI, B., GELLY, G., ACCARD, A., LAFRAGETTE, J.-L., DOUSSIÈRE, P., LAMBERT, M., and FERNIER, B.: '1·55 μm high-gain polarisation-insensitive semiconductor travelling-wave amplifier with low driving current', *Electron. Lett.*, 1990, **26**, pp. 124–125

2 CHA, I., KITAMURA, M., HONMOU, H., and MITO, I.: '1·5 μm-band travelling-wave semiconductor optical amplifiers with window facet structure', *Electron. Lett.*, 1989, **25**, pp. 1241–1242

3 DOUSSIÈRE, P., GARABEDIAN, P., COLSON, V., LEGOUEZIGOU, O., LEBLOND, F., LAFRAGETTE, J. L., MONNOT, M., and FERNIER, B.: 'Polarisation insensitive semiconductor optical amplifier with buried laterally tapered active waveguide'. Proc. Top. Meet. Opt. Amplifiers and Their Applications, Santa Fe, NM, 1992, pp. 140–143

4 BRYANT, E. G., CARTER, S. F., ELLIS, A. D., STALLARD, W. A., WRIGHT, J. V., and WYATT, R.: 'Unrepeatered 2·4 Gbit/s transmission experiment over 250 km of step-index fibre using erbium power amplifier', *Electron. Lett.*, 1990, **26**, pp. 528–530

5 OBERG, M. G., and OLSSON, N. A.: 'Wavelength dependence of noise figure of a travelling-wave GaInAsP/InP laser amplifier', *Electron. Lett.*, 1988, **24**, pp. 99–100

6 BARKER, L. N., HUNTER, C. A., CAMERON, K. H., HEATLEY, D. J. T., DEVLIN, W. J., REGNAULT, J. C., and CALTON, R. L.: 'Packaged semiconductor laser preamplified receiver at 2·4 Gbit/s'. Proc. CLEO, Anaheim, CA, 1990, pp. 310–311

7 OLSSON, N. A., OBERG, M. G., TZENG, L. D., and CELLA, T.: 'Ultra-low reflectivity 1·5 μm semiconductor laser preamplifier', *Electron. Lett.*, 1988, **24**, pp. 569–570

8 GRARD, E., MONNOT, M., DOUSSIÈRE, P., GARABEDIAN, P., LEBLOND, F., LAFRAGETTE, J.-L., JOURNOT, E., GELLY, G., and FERNIER, B.: 'Polarization independent, compact semiconductor amplifier module, with high gain and low consumption'. Proc. ECOC, Paris, France, 1991, pp. 78–80

9 PRESBY, H. M.: 'Near 100% Efficient Fiber Microlenses'. Proc. OFC'92, PD24, San Jose, CA, 1992

10 CHOY, M. M., LIU, K., BAGLEY, M., and O'MAHONY, M.: 'Wide bandwidth multichannel amplification with low crosstalk using a quantum well amplifier'. Proc. CLEO, Anaheim, CA, 1992, pp. 346–347

11 DURHUUS, T., MIKKELSEN, B., and STUBKJAER, K. E.: 'Intermodulation distortion and crosstalk in cascaded laser amplifiers'. Proc. Top. Meet. on Opt. Amplifiers and Their Applications, Monterey, CA, 1990, pp. 196–199

ALGEBRAIC DECODING OF THE TERNARY (11, 6, 5) GOLAY CODE

M. Elia and E. Viterbo

Indexing terms: Codes and coding, Error-correction codes

An algebraic decoding algorithm for the ternary (11, 6, 5) Golay code is presented.

Introduction: Algebraic decoding of cyclic error-correcting codes has recently received considerable attention (see References 1–6). In this letter an algebraic decoding algorithm for the ternary (11, 6, 5) Golay code is presented.

The ternary (11, 6, 5) Golay code: The ternary Golay code is the only perfect code over a nonbinary field that corrects multiple errors [7]. It is a cyclic perfect code over $GF(3) = \{0, 1, -1\}$, with an irreducible generator polynomial $g(x) = x^5 + x^4 - x^3 + x^2 - 1$ that divides $x^{11} - 1$. It is also a ternary quadratic residue code [8]. Let α denote a root of $g(x)$. α is a primitive 11th-root of unity in $GF(3^5)$. Let $\mathscr{C} = \{1, 3, 9, 5, 4\}$ be the cyclotomic coset associated with $g(x)$.

Let $r(x) = c(x) + ux^i + vx^j$ be a received word, where $c(x)$ is a code word and where errors u and v occur at locations i and j with $i \neq j$. If no errors occur then $u = v = 0$. If $u \neq 0$ and $v = 0$ then one error has occurred at location i. Lastly, if two errors have occurred then $u, v \in \{1, -1\}$. We define the syndromes as

$$S_k = r(\alpha^k) = u\alpha^{ki} + v\alpha^{kj}, \qquad k \in \mathscr{C}$$

To correct the errors we must know their magnitudes and locations. In the case of a double error we need four syndromes to obtain four equations. Only one syndrome must be directly computed from $r(x)$, namely S_1, and only two more syndromes give irredundant information, namely $S_5 = S_1^{27}$ and $S_4 = S_1^{81}$. However, the decoding algorithm may be based only on two syndromes S_1 and S_5:

$$\begin{cases} S_1 = u\alpha^i + v\alpha^j \\ S_5 = u\alpha^{5i} + v\alpha^{5j} \end{cases} \tag{1}$$

Substituting $y_1 = u\alpha^i$ and $y_2 = v\alpha^j$, and observing that $u^5 = u$ and $v^5 = v$, for $u, v \in GF(3)$, we obtain the set of equations:

$$\begin{cases} y_1 + y_2 = S_1 \\ y_1^5 + y_2^5 = S_5 \end{cases} \tag{2}$$

with $y_1 = y_2 = 0$ in the case of no error and $y_1 \neq 0$, $y_2 = 0$ in the case of a single error. If a double error occurs, we find y_1 and y_2 as roots of the equation

$$y^2 - \sigma_1 y + \sigma_2 = 0 \tag{3}$$

where $\sigma_1 = y_1 + y_2$ and $\sigma_2 = y_1 y_2$ are elementary symmetric functions related to the syndromes by the Newton identities [1]:

$$\begin{cases} S_1 = \sigma_1 \\ S_5 = S_1^5 + \sigma_2 S_1^3 - \sigma_2^2 S_1 \end{cases} \tag{4}$$

Let us observe that $\sigma_2^{22} = 1$. Therefore, on computing σ_2 from the second equation in (4), we must take the correct determination. The next lemma proves that this choice is not ambiguous.

Lemma 1: Equation

$$\sigma_2^2 - S_1^2\sigma_2 + \frac{S_5 - S_1^5}{S_1} = 0 \tag{5}$$

has only one root that satisfies the condition $\sigma_2^{22} = 1$.

Proof: First we prove that at least one of the roots σ_2' and σ_2'' of eqn. 5 does not satisfy the condition, since, if $\sigma_2'^{22} = \sigma_2''^{22} = 1$ then $\sigma_2'^{22}\sigma_2''^{22} = 1$ and we would have

$$\sigma_2'^{22}\sigma_2''^{22} = \left(\frac{S_5 - S_1^5}{S_1}\right)^{22} = S_1^{88}(S_1^{22} - 1)^{22} = 1$$

In $GF(3^5)$, the power $S_1^{22} = \gamma$ is an 11th root of unity. So the condition

$$\gamma^4(\gamma - 1)^{22} = 1 \tag{6}$$

should hold for an 11th root of unity, therefore $x^4(x-1)^{22} - 1$ should have a common factor with $x^{11} - 1$. Application of the Euclid algorithm shows that these two polynomials are relatively prime; then (6) is not satisfied by any 11th root of unity.

From eqn. 2 it is now straightforward to check that $-S_5 - S_1^5/S_1 = (y_1^2 + y_2^2)^2$, so we have

$$\begin{cases}\sigma'_2 = y_1 y_2 \\ \sigma''_2 = (y_1 - y_2)^2\end{cases} \quad (7)$$

and therefore the first part of the proof excludes the possibility that σ''_2 is a 22nd root of unity. □

Lemma 2: A code word has one error, if and only if $S_5 = S_1^5$, $S_1 \neq 0$.

Proof: If there is precisely one error at location i, then $S_1 = u\alpha^i$, and $S_5 = u\alpha^{5i}$. Since $u^5 = u$ we have

$$S_5 = S_1^5$$

as required.

Conversely if the above condition is satisfied, then the second equation in (4), together with condition $S_5 = S_1^5$, implies that σ_2 is a root of the equation

$$\sigma_2 S_1(\sigma_2 - S_1^2) = 0$$

Then either $\sigma_2 = 0$, which means that only one error occurs, or $\sigma_2 = S_1^2$. The latter is excluded because it gives a double root $y = -S_1$ in (3), which is not compatible. In fact, we have

$$y^2 - S_1 y + S_1^2 = y^2 + 2S_1 y + S_1^2 = (y + S_1)^2 = 0$$

and from $y_1 = y_2 = u\alpha^i = v\alpha^j$ we distinguish two cases: (i) if $u = v$ then $i = j$ and one error u occurs in position i, but this means $y = S_1$, contradicting $y = -S_1$; (ii) if $u = -v$ then $\alpha^i = -\alpha^j$, which is again impossible, since raising this expression to the 11th power gives $1 = -1$. □

A complete decoding algorithm: Let us denote with $L_\alpha(.)$ the discrete logarithm to base α in the cyclic group of the 11th roots of unity. Since the code is perfect, the correction of up to two errors exhausts all possibilities. Therefore we propose the following complete decoding algorithm:

(*a*) If $S_1 = 0$, read out $r(x)$ and end this algorithm; otherwise, go to next step.

(*b*) If $S_5 = S_1^5$, then a SINGLE error

$$u = S_1^{11} \quad \text{occurs in position} \quad i = L_\alpha(S_1^{12})$$

Write out $r(x) - ux^i$ and end this algorithm; otherwise, go to next step.

(*c*) TWO errors occur. From Newton identities obtain the second degree eqn. 5 whose roots are

$$\sigma_2 = -S_1^2 \pm \sqrt{\left(\frac{-S_5 - S_1^5}{S_1}\right)}$$

Choose the root that satisfies the condition $\sigma_2^{11} = \pm 1$ and write the equation

$$y^2 - S_1 y + \sigma_2 = 0$$

The roots of this equation,

$$y_{1,2} = -S_1 \pm \sqrt{(S_1^2 - \sigma_2)}$$

are in GF(3^5) because $S_1^2 - \sigma_2 = (y_1 - y_2)^2$ is a perfect square. Compute the errors as

$$u = y_1^{11} \quad \text{and} \quad v = y_2^{11}$$

and obtain the error locations as

$$i = L_\alpha\left(\frac{y_1}{u}\right) \qquad j = L_\alpha\left(\frac{y_2}{v}\right)$$

Finally write out the received code word as

$$r(x) - ux^i - vx^j$$

Acknowledgment: This work was financially supported by the Politecnico di Torino under internal grant POLI4169-87-Cap.11205.

3rd September 1992

M. Elia and E. Viterbo (*Dipartimento di Elettronica, Politecnico di Torino, I-10129 Torino, Italy*)

References

1 BOURS, P., JANSSEN, J. C. M., VAN ASPERDT, M., and VAN TILBORG, H. C. A.: 'Algebraic decoding beyond e_{BCH} of some binary cyclic codes, when $e > e_{BCH}$', *IEEE Trans.*, 1990, **IT-36**, (1), pp. 214–222
2 ELIA, M.: 'Algebraic decoding of the (23, 12, 7) Golay code', *IEEE Trans.*, 1987, **IT-33**, (1), pp. 150–151
3 HUMPHREYS, J. F.: 'Algebraic decoding of the ternary (13, 7, 5) quadratic residue code', *IEEE Trans.*, 1992, **IT-38**, (3), pp. 1122–1125
4 REED, I. S., TRUONG, T. K., CHENG, X., and YIN, X.: 'The algebraic decoding of the (41, 21, 9) quadratic residue code', *IEEE Trans.*, 1992, **IT-38**, (3), pp. 974–986
5 REED, I. S., YIN, X., and TRUONG, T. K.: 'Algebraic decoding of the (32, 16, 8) quadratic residue code', *IEEE Trans.*, 1990, **IT-36**, (4), pp. 876–880
6 REED, I. S., YIN, X., and TRUONG, T. K.: 'Decoding the (24, 12, 8) Golay code', *IEE Proc. E.*, 1990, **137**, (3), pp. 202–206
7 TIETÄVÄINEN, A.: 'On the nonexistence of perfect codes over finite fields', *SIAM J. Appl. Math.*, 1973, **24**, pp. 88–96
8 MACWILLIAMS, F. J., and SLOANE, N. J. A.: 'The theory of error-correcting codes' (Elsevier, New York, 1976)

RESULTS OF 12GHz PROPAGATION MEASUREMENTS IN LAE (PNG)

Q. W. Pan and G. H. Bryant

Indexing terms: Radiowave propagation, Attenuation, Rainfall rate, Rain-cell diameter, Rain height

Satellite-to-earth propagation attenuation data above 10GHz in the tropical and equatorial areas is scarce due to the fact that most developing countries in this region cannot afford complicated beacon receivers and have limited expertise in this field. There is therefore a lack of data at high elevation angles. At Lae the elevation to AUSSAT is 73 degrees. In the Letter a low-cost and simple system for measuring propagation path attenuation of satellite signals at 12GHz is reported. The novelty of this system is the use of a standard domestic satellite low-noise block (LNB) connected directly to a spectrum analyser in place of an expensive beacon receiver. The rainfall is mainly convective with relatively small rain-cell diameters. A high elevation angle makes it possible, to some extent, to separate the effects of the individual rain cells.

Introduction: In satellite transmission at frequencies above 10GHz, signal attenuation is mainly attributed to rain. Many slant path attenuation prediction models, derived from rainfall rate data accumulated over many years in the temperate region, work reasonably well. However, applying the same models to the tropics, where convective rains are dominant, is not accurate enough. Furthermore, in temperate climates, for the same rainfall rate, the attenuation decreases with the elevation angle. But in the tropics the reverse is found to be the case. This may be due to the comparatively small diameter of convective rain cells. In order to have an appropriate revised model for the tropics, more data from this region should be collected.

Satellite signals: AUSSAT provides, among its services, a beacon at 12·74975GHz and the ABC TV channel at