北京博原科技有限公司 · BOYUAN TECHNOLOGY

半导体 IP 核 · 高性能存储与纠错码（ECC）专家

BCH 编解码器 IP 核
x32bit · GF(2^{13}) 技术白皮书

面向闪存与存算一体的可定制纠错方案

产品 BCH Codec x32bit GF(2^{13})

版本 V1.0

日期 2026 年 10 月

适用 ASIC / FPGA 集成，系统架构与存储可靠性评估

摘要 本白皮书系统介绍博原科技新一代 BCH 编解码器 IP 核。该 IP 工作于 GF(2^{13}) 域，输入/输出数据总线为 32bit，纠错位数与缩短码长度可定制。解码器采用 EDC / KES / CSM 三级流水线，关键方程求解器（KES）并行度可配置，以在面积与吞吐之间灵活权衡。文档涵盖 BCH 码基础、缩短码补零与字对齐规则、编解码器架构、AXI-Stream 接口、验证方法、SMIC 28nm 综合结果，以及在存算一体（CIM）芯片中的应用。

© 2026 北京博原科技有限公司 | www.bjbytech.com | sale@bjbytech.com | 电话 / 微信（同号）13601005061

目录

1 存储可靠性的新挑战

2 BCH 码基础与 GF(2^{13})

3 缩短码的补零与字对齐规则

4 编码器架构与 AXI-Stream 输入对齐

5 解码器：EDC / KES / CSM 三级流水线

6 KES 并行度可定制：面积与吞吐权衡

7 AXI-Stream 接口与结果上报

8 测试与验证方法

9 综合结果与频率口径

10 存算一体（CIM）应用

11 结论与联系方式

1 存储可靠性的新挑战

1.1 闪存的错误来源

NAND 闪存随着工艺微缩、单元多级化（SLC → MLC → TLC / QLC）以及 3D 堆叠层数增加，原始比特错误率（RBER）持续上升。主要错误来源包括：单元间干扰（cell-to-cell interference）、编程/擦除循环造成的氧化层磨损、读干扰（read disturb）、数据保持（data retention）随时间的电荷泄漏，以及工艺偏差。纠错码（ECC）是闪存控制器中保证数据完整性的核心模块，其纠错能力直接决定存储器的寿命（ endurance）与数据保持时间。

1.2 存算一体带来的新需求

在存算一体（Compute-in-Memory, CIM）架构中，存储阵列直接参与乘加运算，权重与激活数据常驻于片上存储。工艺偏差、电源噪声与器件老化更易引起权重比特翻转，而错误权重会直接传播到计算阵列，造成推理结果的系统性偏差。因此 CIM 芯片需要**低时延、可在线运行**的纠错能力，并能按阵列带宽与面积预算灵活配置。

> **本 IP 的定位**
> 博原 BCH 编解码器 IP 以 32bit 数据总线、可定制纠错能力与面积高效的流水线架构，同时服务于传统闪存/SSD 纠错与新兴的存算一体存储阵列保护。

2 BCH 码基础与 GF(2^{13})

2.1 伽罗华域 GF(2^{13})

BCH 码建立在有限域 GF(2^m) 之上。本 IP 取 m = 13，即 GF(2^{13})，域元素个数为 2^{13} = 8192，对应的本原 BCH 码最长码字为 n = 2^{13} − 1 = **8191 bit**。选择 m = 13 使得单码字可覆盖 512 Byte（4096 bit）级别的数据块并留有足够的校验位余量，是闪存与片上存储应用中常见的平衡点。

2.2 本原 BCH 码与缩短码

对于一个能纠正 t 个随机错误的本原 BCH 码，其生成多项式 g(x) 由 $\alpha, \alpha^2, \ldots, \alpha^{2t}$ 的最小多项式的最小公倍式构成，设计最小距离为 2t + 1。编码时将信息多项式 m(x) 乘以 x^{n-k} 后对 g(x) 取模得到校验位。解码则分为三步：由接收码字计算伴随式，求解关键方程得到错误位置多项式，再通过搜索确定错误位置并完成纠正。

实际系统的数据块长度往往小于本原码长。**缩短码**通过固定若干高位信息位为零（发送端不发送、接收端不解码这些位），在保持纠错能力 t 与校验位长度不变的前提下，把码字缩短到所需长度。本 IP 的信息位长度与码长均可定制，典型配置如下。

参数	16bit 纠错配置	36bit 纠错配置
纠错能力 t	16 bit	36 bit
信息位长度 k	4096 bit（512 Byte）	4136 bit
校验位长度	208 bit	468 bit
码字长度 n	4304 bit	4604 bit
伽罗华域	GF(2^{13})	GF(2^{13})

校验位与码字长度依据哥拉夫域阶数、纠错能力与缩短量确定；其他纠错等级与信息位长度可定制。

3 缩短码的补零与字对齐规则

当数据以 32bit 字（dim = 32）为单位输入输出时，信息位长度未必是字长的整数倍，校验位长度亦然。若不对齐，字边界会随帧漂移，导致后级模块无法用统一规则处理。本 IP 的对齐规则如下。

3.1 信息位高位补零

设信息位长度为 `message_length`，扩展到字边界所需的字数为 `message_dw = ceil(message_length / dim)`，则在信息矩阵**第一行（最高位端）的前 `mask_bit` 个位置补零**：

```
mask_bit = message_dw × dim − message_length
Message(1, 1 : mask_bit) = 0 // 高位端补零，低位端对齐
```

补零置于高位端而非低位端，是因为缩短码的语义等价于"本原码的高位信息位为零"；这样解码输出时只需丢弃前导零字即可恢复原始信息，无须额外的数据搬移。

3.2 校验位对齐与全零首字的消除

校验位长度为 `par_bit` 时，同样补零到字边界：

```
bzp = dim − rem(par_bit, dim)
m1(1, 1 : bzp) = 0 // 校验位高位补零
Code = m2(2 : end, :) // 去掉第 1 行全 0 字
```

> **设计要点**
> 补零后产生的第一行为全 0 字，若送给解码器不携带信息，属于冗余传输。本实现将其从码字中去除（`Code = m2(2:end,:)`），既节省带宽，也保证编码与解码两端字边界严格一致。

4　编码器架构与 AXI-Stream 输入对齐

4.1　LFSR 除法编码

编码器采用基于生成多项式 g(x) 的线性反馈移位寄存器（LFSR）实现多项式除法：信息位逐位/逐字移入寄存器组，按 g(x) 的系数进行异或反馈；信息位全部移入后，寄存器中剩余内容即为校验位。该结构面积小、规则性强，便于参数化生成不同码长与纠错等级。

4.2　编码器输入数据对齐规则

设输入数据位宽 DW = 32，消息总位数 MSG_BITS。由于最后一拍通常不足一个完整字，编码器需要明确"每一拍的哪些 bit 是有效消息"。定义：

```
LAST_BITS = MSG_BITS mod DW // 余数为 0 时取 DW
NW = ceil(MSG_BITS / DW) // 总拍数
LW = NW - 1 // 最后一拍序号
BUF_BITS = DW - LAST_BITS // 需要从上一拍缓存的位数
```

数据组装规则为：

- **非末拍**：{tdata_buf, s_axis_tdata[DW−1 : DW−LAST_BITS]}——取输入字的高 LAST_BITS 位，与上一拍缓存拼接。
- **末拍**：{tdata_buf, s_axis_tdata[LAST_BITS−1 : 0]}——取输入字的低 LAST_BITS 位，与缓存拼接后凑满一个字。

其中 `s_axis_tlast` 标识输入帧的最后一拍，`s_axis_tuser` 标识帧起始。收发双方按上述规则即可在任意 MSG_BITS 下保持字对齐，无须额外的长度协商。

5　解码器：EDC / KES / CSM 三级流水线

解码器由三个子模块构成，并以流水线方式调度，使得三个数据帧可同时处于不同解码阶段：



5.1 EDC：伴随式计算

EDC 对接收码字 r(x) 在 α^1 … α^{2t} 处求值得到 2t 个伴随式 $S_i = r(\alpha^i)$。若全部为零则判定无误码；否则将伴随式送入 KES。EDC 每周期处理一个 32bit 字，延时约为 `ceil(N/32)` 周期（N 为码字长度）。

5.2 KES：关键方程求解

KES 由伴随式求解关键方程，得到错误位置多项式 σ(x)。实现采用迭代结构，共迭代 2t 次，每周期处理 U 个错误位置（U 即展开因子，见第 6 节），延时约为 `ceil(2t/U)` 周期。这是解码器中计算最密集、面积占比最高的模块，也是本 IP 可定制性的核心所在。

5.3 CSM：Chien 搜索与纠错

CSM 逐位置检验 σ(x) 的根以确定错误位置，并对二进制 BCH 码完成比特翻转纠正。CSM 采用博原科技的专利技术，以面积高效的方式实现，每周期处理一个 32bit 字，延时约为 `ceil(N/32)` 周期。其实现的关键在于迭代边界的精确推导：搜索次数需由码长、纠错能力与域参数严格计算，边界的偏差（多一次或少一次迭代）会导致仿真与硬件行为不一致。

5.4 流水线的吞吐与时延口径

> **时延定义**
> 解码时延定义为**从最后一拍输入有效（TVALID & TREADY）到第一拍输出有效**的周期数。三级流水线稳态下每级处理一帧，因此吞吐由最慢一级决定，而单帧时延取决于三级各自的延时之和及级间寄存。EDC/CSM 约 ceil(N/32) 周期，KES 约 ceil(2t/U) 周期；设计时将 KES 的 U 配置为使三级延时大致匹配，可获得连续不空转的输出。

6 KES 并行度可定制：面积与吞吐权衡

KES 的展开因子 U 表示每周期并行处理的错误位置数。U 越大，迭代次数 `ceil(2t/U)` 越少、KES 延时越低，但并行硬件资源与面积随之增加。这一旋钮使同一架构能覆盖不同应用：

纠错等级	KES 结构	特点
16bit（t = 16）	半展开（half-unrolled）	2t 远小于数据拍数，以适度并行平衡三级周期，面积友好
36bit（t = 36）	全并行（fully parallel）	2t 已接近数据拍数，迭代充分展开避免 KES 成为瓶颈，吞吐优先

KES 展开度的选择取决于纠错能力与数据拍数的相对关系，目的是使三级流水线各级的处理周期相互匹配：

- **16bit 纠错（t = 16，2t = 32）**：2t 远小于码字的数据拍数 `ceil(4304/32) ≈ 135`，KES 计算量相对较小。采用**半并行展开**即可满足流水线节奏，无需全并行带来的面积开销，从而以更经济的资源平衡三级的处理周期。

- **36bit 纠错（t = 36，2t = 72）**：2t 已接近数据拍数 `ceil(4604/32) ≈ 144` 的量级，KES 计算量显著增大。采用**全并行结构**将迭代充分展开，把 KES 单帧处理周期压缩到与 EDC/CSM 相当，避免 KES 成为瓶颈。正因如此，即便纠错能力接近翻倍，解码器仍可在 1GHz 时钟约束下收敛——这正是"36bit 全并行"而非简单提高 t 的设计价值。

> **可定制项**
> 纠错位数、信息位长度、码字长度与 KES 展开因子 U 均可定制。客户可按阵列带宽、存储容量、目标工艺与面积预算选择合适的组合。

7　AXI-Stream 接口与结果上报

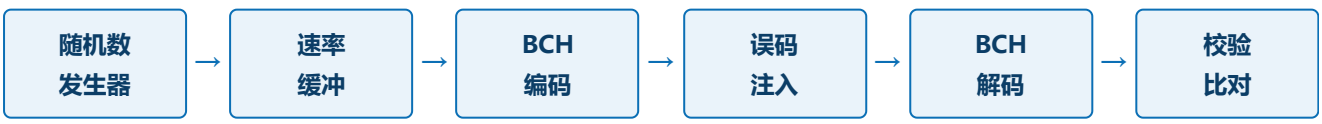
编解码器顶层采用标准 AMBA AXI-Stream 接口，输入/输出均为 32bit，通过 TVALID / TREADY 握手传输数据，接收端可通过拉低 TREADY 施加背压，便于与片上总线或 CIM 宏直接对接。

信号	方向 / 位宽	说明
s_axis_tdata / tvalid / tready	Input / 32,1,1	输入数据总线与握手
s_axis_tuser / tlast	Input / 1,1	输入帧起始 / 帧结束标志
m_axis_tdata / tvalid / tready	Output / 32,1,1	输出数据总线与握手
m_axis_tuser	Output / 2	Bit[0] 输出帧起始；Bit[1] 输出校正标志
m_axis_tlast	Output / 1	输出帧结束标志
dec_result	Output / 8	Bit[6:0] 纠错位数；Bit[7] 解码成功标志
dec_result_en	Output / 1	解码结果有效，按帧输入顺序汇报

其中编码器端口为 12 个信号，解码器端口为 14 个信号；`dec_result` 与 `dec_result_en` 使系统能逐帧获知纠错位数与解码成败，可用于磨损均衡、可靠性统计与在线诊断。

8　测试与验证方法

IP 提供完整的自检测测试平台，覆盖 RTL 仿真与 FPGA 板级实测两种形态。数据通路如下：



- **随机数发生器**采用 4 路线性反馈移位寄存器（LFSR）并行结构，输出 32bit 伪随机数据。
- **速率缓冲**完成跨时钟域与速率匹配，使激励稳定送入编码器。
- **误码注入**的位置、图案与使能源自可配置寄存器，可覆盖不同纠错等级与错误分布（随机错误、突发错误、边界错误）。
- **校验比对**逐帧比对原始数据与译码输出，统计通过/失败帧数并报告纠错位数。

在 FPGA 实测中，测试平台集成于顶层，通过 VIO 在线配置错误图案与帧使能，实时监测解码结果与帧计数，可长时间连续运行以统计纠错性能。

9　综合结果与频率口径

9.1　综合条件

在 SMIC 28nm 工艺库（scc28nhkcp_vhsc35p140_rvt_tt_v0p9_25c_basic）下，于 TT 典型工艺角（0.9V / 25°C）对解码器内核进行 DC 综合，时钟约束为 1ns（1GHz）。

9.2　结果数据

项目	16bit @ 4304bit	36bit @ 4604bit
设计	bch_4304_4096_dec_core	bch_4604_4136_dec_core
端口数	19,592	43,312
网络数	70,950	171,337
单元数	51,458	128,240
组合逻辑单元	40,361	108,060
时序逻辑单元	11,020	19,987
Buf / Inv	5,595	14,486
总单元面积	84,755.16	199,570.40

面积单位：工艺库标准单位。Buf/Inv 面积含于组合逻辑面积；未指定线负载模型，Net Interconnect Area 与 Total Area 为 undefined。

9.3　面积差异分析

36bit 配置的单元数约为 16bit 的 2.5 倍，这是可预期的：伴随式数量由 2t 决定（32 → 72），KES 采用全并行结构使并行数据通路成倍增加，CSM 的搜索与纠正通路也随 t 扩展。需要说明的是，用单元数直接比较不同工艺、不同约束下的实现并无意义；本表仅用于说明同一工艺与约束下两种纠错等级的相对代价，也为客户按面积预算选择纠错等级提供依据。

> **频率口径声明**
> 上述结果为 DC 综合阶段的预估，未计入布局布线后的互连延迟，**不代表最终签核（sign-off）频率**。1ns 约束下综合收敛意味着时序裕量在综合阶段刚好满足，进入 P&R 后仍有裕量被互连延迟消耗的风险，建议在具体工艺与布局下重新评估。

10　存算一体（CIM）应用

在 CIM 芯片中，本 IP 可用于权重与激活存储的软错误在线纠错：三级流水线对每个存储块的码字进行低时延解码，避免错误权重传播到乘加阵列；32bit AXI-Stream 接口便于与 CIM 宏及片上总线对接；纠错位数、码长与 KES 并行度均可按阵列带宽、存储容量与面积预算定制，兼顾可靠性与能效。

> **集成建议**
> 对面积受限的边缘推理阵列，可选用较低纠错等级与半展开 KES；对高密度权重存储或生命末期可靠性要求高的场景，可选用 36bit 全并行配置以获得更高纠错能力与吞吐。

11　结论与联系方式

博原 BCH 编解码器 IP 以 32bit 数据总线、GF(2^{13}) 域、可定制纠错与码长、面积高效的三级流水线以及可配置的 KES 并行度，在闪存/SSD 与存算一体应用中提供了可靠性、面积与吞吐之间的灵活平衡。成熟的定义、完整的验证平台与 SMIC 28nm 综合数据，可降低 IP 集成风险并缩短产品上市时间。

联系我们 • 购买 / 评估 / 技术咨询

销售 / 评估： sale@bjbytech.com　　**电话 / 微信（同号）：** 13601005061

技术咨询： tech@bjbytech.com　　**电话 / 微信（同号）：** 13601005061

网站： www.bjbytech.com

© 2026 北京博原科技有限公司。本白皮书内容如有更新，恕不另行通知。文中综合数据为特定工艺与约束下的预估结果，不构成最终性能承诺。